



Navigating Cross-Border Data Flows and the GDPR

Trade policy recommendations

2025



Preface

Cross-border data flows are the lifeblood of our interconnected global economy and are a key part of everything from the development of new AI tools to managing the global value chains of the traditional manufacturing industry. However, they also present significant regulatory challenges, particularly in aligning the free flow of data with robust frameworks like the GDPR. At the National Board of Trade, we are dedicated to exploring how trade policies can adapt to the challenges of the digital age while fostering sustainable economic growth.

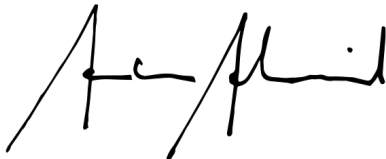
This study examines the interplay between data governance and international trade. We aim to identify the barriers businesses face in navigating the fragmented regulatory landscape of cross-border data flows, and present actionable recommendations to reduce these barriers.

Our recommendations are designed to be GDPR compliant, as well as respect that countries have different views on the balance between economic growth and the need to protect data for reasons of privacy, economic development or security.

We believe that striking the right balance between facilitating data flows and maintaining high standards of data protection is both necessary and achievable. This report offers insights and recommendations aimed at policymakers seeking to protect data while fostering economic growth and digital innovation.

This study has been written by Isaac Ouro-Nimini Hansen, with advice, comments and contributions from Emma Sävenborg, Olivier Linden, Sophia Lara and Hannes Lenk.

Stockholm, February 2025



Anders Ahnlid
Director-General
National Board of Trade Sweden

Executive summary

Cross-border data flows are essential to the modern digital economy, underpinning products and services from e-commerce to artificial intelligence, and the economic importance of digital trade has brought cross-border data flows to the forefront of international policy discussions.

However, a fragmented regulatory landscape and varying interpretations of data protection laws have created significant barriers to the free flow of data, to trade and to the many benefits of digitalisation.

This study explores these challenges from a trade policy perspective, including a background on the underlying issues, and provides targeted recommendations to mitigate barriers to cross-border data flows. By focusing on useful, realistic and incremental improvements, our study outlines ways to enhance the predictability and efficiency of data transfers while respecting the need to regulate. Our approach to this is global in scope, but our focus is European, by ensuring that the options we evaluate align with the GDPR. We want our recommendations to be valuable, not only to businesses, business associations and policymakers in the EU, but also to those outside of it.

Building on an analysis of the current regulatory landscape, the study's recommendations include:

- Developing standardised definitions for key concepts such as "personal data" and "adequate protection" to harmonise legal interpretations and reduce ambiguities.
- Accelerating the EU's adequacy decision process to expand trusted data-sharing frameworks and facilitate digital trade.
- Supporting developing economies through capacity-building initiatives and technical assistance to help align their data protection frameworks with global standards.
- Establishing a "Data Flows Test" for EU policymaking to ensure that new regulations are assessed for their impact on data transfers and to minimize unnecessary trade restrictions.
- Improving regulatory transparency by drawing inspiration from the WTO system, and by providing SME-friendly information platforms.

These recommendations have been designed to help policymakers balance the economic growth and innovation that depend on seamless cross-border data exchanges, with other data-related concerns, paramount of which is the protection of personal data.

Each recommendation has been evaluated for its feasibility, usefulness and compatibility with the GDPR. While not offering a complete resolution to global data flow challenges, by addressing these criteria, we aim to offer a roadmap for how to reduce regulatory fragmentation, encourage global cooperation, and strengthen the digital economy.

Table of contents

Preface	2
Executive summary	3
Table of contents	4
1 Introduction	5
1.1 Methods	7
1.2 Scope and definitions	10
1.2.1 Data flows	10
1.2.2 Personal vs. non-personal data	10
1.2.3 Data subject and data handler	11
2 Data flows	12
2.1 The global importance of cross-border data flows	12
2.2 Regulating cross-border data flows	14
2.2.1 The need to regulate	14
2.2.2 Regulatory options	16
3 The GDPR	21
3.1 Cross-border data flows per the GDPR	22
3.2 The GDPR test	23
4 Challenges	25
4.1 The challenge of complying with the GDPR	25
4.2 A global patchwork problem	28
4.3 Economic inefficiencies	29
4.4 The cost of technological advancements	31
5 Recommendations	33
5.1 Convergence around a common terminology	33
5.2 More, and faster, adequacy decisions	34
5.3 Technical assistance and capacity-building	36
5.4 A ‘Data Flows Test’	37
5.5 Transparency of regulations	39
6 Concluding remarks	41
References	42
Sammanfattning på svenska Summary in Swedish	45

1 Introduction

The flow of information across borders, what we refer to as cross-border data flows, is an essential part not only of our modern economy – but also our modern lives. This exchange of data between individuals, companies and authorities has enabled everything from e-democracy to e-commerce, from political revolutions to telemedicine.

For consumers, these data flows translate into access — access to products, services and a wealth of knowledge. For business, in all sectors of the economy, cross-border data flows are crucial. More than half of all businesses worldwide rely on cloud computing, and data flows enable everything from research, to production, to after-sales services. Digital trade already accounts for more than half of all services exports globally, and could account for almost one quarter of the global GDP.¹

From a purely trade policy perspective, data flows represent trade in and of itself. Streaming services or telemedicine, for example, are built on data flowing across borders. But data flows are also a key part of many initiatives that enable and facilitate trade and can simplify the often cumbersome realm of customs procedures. Electronic documentation and digital transactions enabled by these flows enhance the efficiency of customs clearance, reducing the time and resources traditionally consumed by paperwork.

These developments are not without their challenges, however. Some of them receive relatively little attention from policymakers dealing with digital trade, such as environmental concerns about the manufacturing of necessary hardware and the growing power demands of digital connectivity. Other challenges, such as data privacy and national security, have become issues of such great importance and concern that specific policy frameworks have been built around them.

Attempts to address these issues have resulted in a vast – and growing – patchwork of regulations on the national and global level, covering the various aspects of cross-border data flows.

This patchwork contains almost the entire spectrum of potential regulatory options. There are some jurisdictions in which the cross-border transfer of data is virtually unregulated, other jurisdictions in which operators are expected to self-regulate, and some jurisdictions – such as the European Union and the European Economic Area (EU)² – where cross-border data flows are strictly³ regulated by public authorities.

These competing – and often incompatible – regulatory options are championed by governments through national legislation, as well as trade and digital agreements at all levels. Perhaps most prominently, the EU has seen some success in spreading its privacy-centric approach, exemplified in the General Data Protection Regulation (GDPR)³.

A government's ability to regulate the digital space is of great concern to citizens, especially regarding online privacy and the protection of personal data. Add to this an unwillingness to delegate regulatory powers to international bodies and the fact that not every society will reach the same conclusions when weighing commerce against privacy

-
1. World Economic Forum (WEF), *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows* (2023).
 2. We use the shortened form "EU" throughout this study, though the term should be understood to also include the EEA, unless otherwise stated.
 3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).



(or national security), and it seems highly unlikely that a single regulatory option will prevail globally. This fragmented regulatory landscape will then remain difficult to navigate, especially for small and medium-sized enterprises (SME) that may lack the resources to hire dedicated expertise.

Regulatory fragmentation and barriers to cross-border data flows blunt the economic benefits of digital connectivity, leading to increased costs and lost opportunities for business, limiting access and choice for consumers. The challenge for policymakers around the world lies in finding ways to mitigate the negative effects of restrictions on cross-border data flows, to better harness the sizeable opportunities offered by digitalisation, while responding to the need to protect data for reasons of privacy, economic development or security. For policymakers in the EU specifically, the right to privacy enshrined in EU law puts serious restrictions on what can be done to facilitate cross-border data flows.

The purpose of this study is to present and analyse different pathways forward for policymakers (primarily in the EU) dealing with digital trade, pathways that could mitigate the challenges facing businesses because of the fragmented, complex and restrictive regulatory landscape that governs cross-border personal data flows. Our outlook is global – in that we are looking at options that can mitigate cross-border issues – but our perspective is European, as we are looking at options that are not obviously incompatible with the GDPR. Hopefully, our recommendations should also be of interest to businesses and business associations, as well as policymakers outside of the EU.

This introductory chapter will describe the purpose, scope and methodology of the study in greater detail and define important terms used throughout the study.

The background chapters that follow contain information on the economic and societal importance of cross-border data flows, on different regulatory approaches, and on the GDPR.

Chapter 4 contains our analysis of the current regulatory situation for cross-border data flows, and the associated issues. Chapter 5 presents several options for moving forward, while staying within the constraints of the GDPR.

Finally, in Chapter 6, we offer a few concluding remarks.

1.1 Methods

To be able to present different options for moving forward, we begin by identifying and describing the current regulatory situation for cross-border data flows, and the challenges that businesses face as a result of these regulations.

We then use the term ‘**recommendations**’ to describe the options for moving forward that we advocate, whilst acknowledging that there is no option that is likely to completely address all the challenges, in the sense that it would be able to remove all the negative effects borne by businesses. Rather, our focus is on options that mitigate the negative effects and thus improve the situation for businesses.

We deem an option to have a mitigating effect if it would address issues that we have identified as problematic in relation to cross-border data flows. As the problems with cross-border data flows are global in nature, for any measure to make a real contribution it must also be something that could realistically be implemented in different regulatory regimes across the globe, including in the EU.

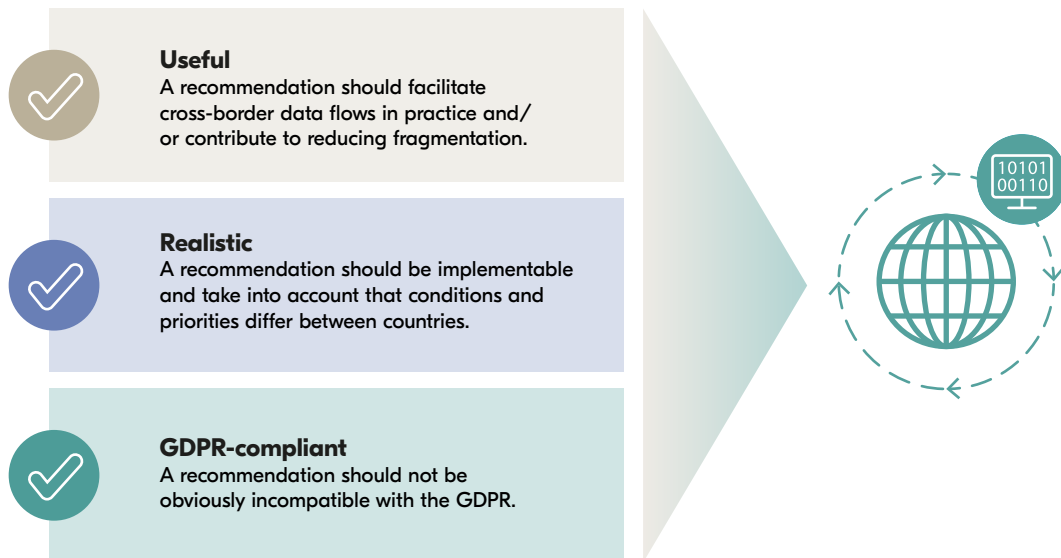
Our criteria for a recommendation can be summed up with the following three points, which will be included in the analysis of each recommendation that we present:

- **Useful.** A recommendation should attempt to address issues that businesses have identified as problematic in relation to cross-border data flows. As will be detailed in Chapter 4, these include: regulatory fragmentation, lack of transparency and clarity regarding the regulations, and the cost of compliance. A question is then asked for each recommendation: *would it facilitate cross-border data flows in practice and/or does it contribute to reducing fragmentation?* The answer will not always be clear, and where there is uncertainty, we have erred on the side of boldness.
- **Realistic.** Any recommendation also needs to be realistic, in that it could feasibly be implemented within the prevailing trade policy landscape.

One *theoretical* recommendation to address many of the problems businesses face with cross-border data flows would be if all members of the World Trade Organization (WTO) agreed to implement data privacy legislation that was similar to the GDPR, and then also submit to the primacy of EU law in matters regarding the protection of personal data.

However, global harmonisation on such a level is an unrealistic scenario. As detailed in Chapter 2.2, countries have different views on the balance between economic development, privacy, free speech, national security, and other concerns that require data flows to be regulated. It is our view that any recommendation needs to take into account the fact that both conditions and priorities differ – and will continue to differ – between countries. This is especially true for developing countries, where the stringent privacy-centric approach favoured by the EU might limit access to monetizable data, or a similarly strict approach that limits cross-border data flows might be necessary to ensure data provides value on a domestic level.

Figure 1. Criteria for recommendations



- **GDPR compliant.** The EU approach to prioritizing between the different aspects of data flows is expressed most prominently in the GDPR.

The adoption of the GDPR has created a conundrum for the EU and its member states. The EU economy is digitalised and EU businesses face many of the challenges detailed in Chapter 4 when it comes to cross-border data flows. Given that many of these challenges spring directly from the disjointed state of data flow regulations across the globe, the natural avenue for the EU would be to seek regulatory coherence on data flows through international commitments.

However, the GDPR strictly limits just what commitments the EU and its member states can agree to when it comes to facilitating cross-border data flows.

Outside of the EU – and outside of these limitations – harmonisation is already happening. Plurilateral agreements are in place, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) that include rules on cross-border data flows, regional initiatives such as the Cross-Border Privacy Rules (CBPR)⁴ of the Asia-Pacific Economic Cooperation (APEC) that enable interoperability and mutual recognition of data protection and online privacy standards, and business-level solutions such as digital trustmarks that promote harmonisation, to name just a few.

What these aforementioned initiatives have in common is that they are either incompatible with the GDPR, or the requirements of the GDPR mean that they would have no real effect as a recommendation to address the challenges of cross-border data flows, at least not for businesses operating in the EU. As such, they are also outside the scope of this study.

4. Infocomm Media Development Authority (Singapore), 'About APEC Cross Border Privacy Rules (CBPR)', accessed 21-04-24 and Organisation for Economic Co-operation and Development (OECD), Digital Trade Inventory – Rules, Standards and Principles (2021).

Instead, we look at the challenges of cross-border data flows from an EU perspective, meaning any recommendation we propose should operate within the limitations of the GDPR. The alternative would be to forego the integration of around 17 per cent of the global economy and one of the largest markets in the world.

Although the limitations of the GDPR are not always clear (as the recent judgments from the Court of Justice of the European Union (CJEU) on the GDPR, Schrems I⁵ and Schrems II⁶, illustrate), for the purposes of this study, any recommendation should not be *obviously incompatible* with the GDPR.

We aim to accomplish this through a desk study, where our contribution lies in summarizing and analysing previous studies on cross-border data flows, as well as applying our own experience and knowledge to offer recommendations, both new and old.

The regulation of cross-border data flows is a fairly well-researched subject, with numerous studies from the Organisation for Economic Co-operation and Development (OECD), the World Economic Forum (WEF) and UN Trade and Development (UNCTAD). We also rely on previous studies published by the National Board of Trade that look at the importance of cross-border data flows for companies based in Sweden, as well as for Swedish multinationals. The business perspective, which is key to this study, is well represented through interviews and surveys conducted by other organizations and by ourselves in previous studies. These surveys and interviews feature businesses from a wide range of sectors, from app developers to companies active in traditional manufacturing sectors.

Online databases hosted by consulting firm McKinsey & Company and law firms Baker McKenzie and DLA Piper have been used to find information about the regulations that govern cross-border data flows in different countries around the world.

Finally, this study uses a trade policy perspective, in both identifying the challenges and offering recommendations. It is worthwhile noting that there are many other perspectives that could be applied. For example, issues related to cross-border data flows are also discussed under the auspices of the United Nations, primarily from a privacy and human rights perspective. However, both the discussion and the development of international *measures* on cross-border data flows continue to take place primarily in the context of trade policy.

Figure 2. Our method



5. Case C-361/14 Maximilian Schrems vs. Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

6. Case C-311/18 Data Protection Commissioner vs. Facebook Ireland Limited and Maximilian Schrems [2020] ECLI:EU:C:2020:559.

1.2 Scope and definitions

Digitalisation, and consequently data flows, permeate nearly every aspect of contemporary life, especially when these terms are understood in their broadest application. Their omnipresence underscores the complexity and the challenge of fully comprehending these broad concepts without any clear boundaries and precise definitions. It is therefore necessary to limit the scope of a study such as this. In this section we will detail and provide reasons for the limitations we have chosen and explain some key terminology used in the study.

1.2.1 Data flows

In a technical context, *data flows* refers to the organized movement of digital information from one point to another, within and across information systems. These flows encompass the transmission of various types of data such as text, images, videos or structured datasets. The process of data ‘flowing’ typically involves the exchange of information between hardware components and software applications, facilitated by established protocols such as the Internet Protocol (IP).

In the case of *cross-border data flows* we are referring to ‘data flows’ in the sense of data flowing from a system (hardware or software) in one country to a system in another country. In our interconnected world, cross-border data flows are not strictly a bilateral issue, as data transmitted from one country to another may flow through systems in multiple intermediate countries.

Our study is entirely focused on this **cross-border aspect** of data flows, along with related challenges and opportunities. While many aspects related to data flows share the same or similar challenges to those raised in this study, we recognize that there may be unique issues regarding the collection, systematization and storing of data (including personal data). We will not delve into such issues.

1.2.2 Personal vs. non-personal data

Regulations on cross-border data flows usually differentiate between personal data (data that contains information related to an identifiable person) and non-personal data, the latter often being defined as everything that is *not* considered personal data⁷. Generally, regulations on the cross-border transfer of non-personal data are significantly less restrictive than those governing personal data. This is especially true in privacy-centric jurisdictions like the EU.

However, the regulatory distinction between personal and non-personal data is often blurred and the common approach of businesses is to err on the side of caution.

Many forms of online activity might seem anonymous at first glance, as the user is not required to directly divulge personally identifiable information (PID)⁸. However, information collected online can still reveal details which, especially when collated, turn non-personal data into personal data. As an example: most cross-border data flows contain ‘metadata’ such as IP or email addresses. These types of data (again, especially when collated) can be considered personal data in some jurisdictions, meaning that a packet that almost entirely comprises non-personal data would still be personal data for regulatory purposes, as it contains metadata.

7. WEF, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows (2020).

8. Any and all data related to an identifiable person can be considered PID, and this could range from official data such as name or financial information, to user-generated content such as photos or comments, to locational data such as coordinates or IP addresses.



The option to turn non-personal data into personal data in this manner will only become more widespread in the future as a result of the ever-increasing processing capabilities of computer hardware.⁹ Failing to comply with regulations on the cross-border flow of personal data can lead to significant financial penalties, which makes businesses even more likely to classify non-personal data as personal data, out of an abundance of caution.¹⁰

As the cross-border flow of non-personal data is less restricted in most countries, it would be easier and more straightforward to find global solutions that would facilitate the cross-border flow of non-personal data, were it not for the practical and legal difficulties in separating non-personal data from personal data we have illustrated.

All of this means that the regulations that govern the cross-border flow of personal data also impact the cross-border flow of non-personal data to a large extent. Any recommendation that would facilitate the cross-border flow of personal data would then incidentally improve the flow of non-personal data. Thus, in this study, we focus on the regulation of the cross-border flow of personal data.

1.2.3 Data subject and data handler

For the sake of simplicity, we have chosen to use the terms ‘data subject’ and ‘data handler’, although there are many different terms used in the various pieces of legislation around the world that govern the cross-border flow of personal data.

The **data subject** is the *person* in “personal data”, the individual who can/could be identified using the personal data.

The **data handler** is just that, the entity (for the purposes of this study, usually the business) that is, according to the applicable laws, handling the data. In most scenarios presented in this study, the data handler will be the entity that wants to send personal data across the border.

9. Mattoo Aaditya and Meltzer Joshua P, ‘International Data Flows and Privacy: The Conflict and Its Resolution’, *Journal of International Economic Law*, vol 21, no 4 (2018) and OECD, Digital Trade Inventory.

10. Mattoo and Meltzer, ‘International Data Flows and Privacy’.

2 Data flows

2.1 The global importance of cross-border data flows

In our current digital era, the global economy is increasingly reliant on cross-border data flows as they form the backbone of modern production, international trade and economic growth. As we continue into the Fourth Industrial Revolution, data flows emerge as not only fundamental to our present economic structures but also to our future economic growth.

The economic importance of these cross-border data flows cannot be overstated. No less than 70 per cent of the anticipated new value created in the global economy during the next decade is expected to hinge on digitally-enabled platform business models.¹¹ In 2022, digital trade¹² already accounted for 54 per cent of total services exports globally, growing faster than any other sector of international trade, and contributing more to global economic growth than trade in goods.¹³ By 2025, the digital economy is expected to account for 24 per cent of global GDP.¹⁴ The increasing importance of cross-border data flows for future economic growth is further underscored by the concomitant exponential growth in global data traffic, which reached 230 billion gigabytes per month in 2020 and is forecast to reach three times that amount by 2026.¹⁵ To put these growth numbers in perspective: as early as 2015 the amount of data transferred across the internet *every second* was higher than the total amount of data available in its entirety on the internet in 1995.¹⁶

Businesses worldwide, with more than 50 per cent of them relying on data flows for cloud computing, leverage data flows across the entire value chain. From research and development to sourcing, production, marketing and after-sales services, data flows enable companies to participate seamlessly in global value chains, making both products and processes more efficient and flexible.¹⁷ It has been estimated that in 2023, the value of business-to-business (B2B) digital cross-border trade alone reached USD 1.78 trillion.¹⁸

11. WEF, From Fragmentation to Coordination.

12. This definition used by the WTO includes all trade that is either digitally ordered or digitally delivered.

13. The International Monetary Fund, OECD, the United Nations, The World Bank and the World Trade Organization (WTO), Digital Trade for Development (2023).

14. Digital Policy Alert, Data Governance Regulation in the G20 – A Systematic Comparison of Rules and Their Effect on Digital Fragmentation (2023).

15. WEF, Data Free Flow with Trust.

16. National Board of Trade (NBT), No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies based in Sweden (2014).

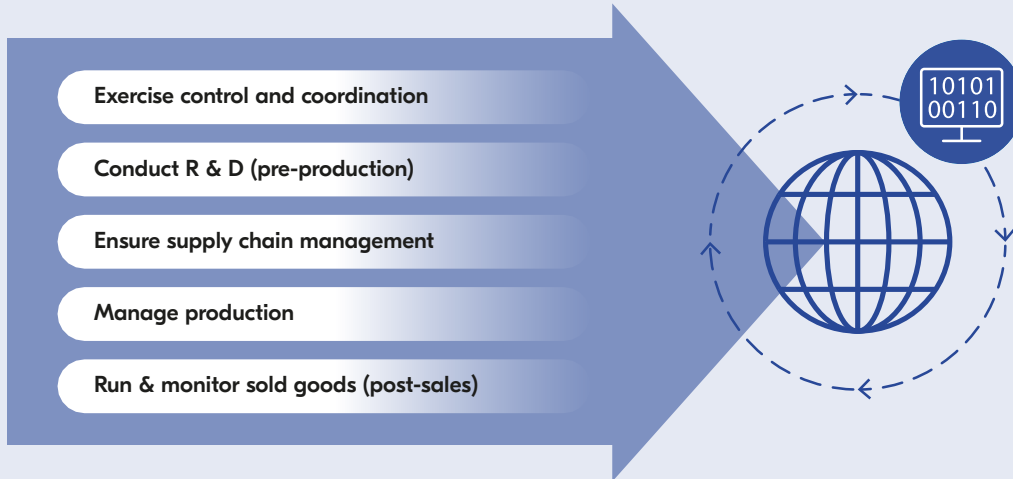
17. Congressional Research Service, Data Flows, Online Privacy and Trade Policy (2020).

18. Hamilton Daniel S. and Quinland Joseph P., the Transatlantic Economy 2021 (2021).

Box 1. Data flows in use

In our modern world it is virtually impossible to do business on even the smallest scale without using data flows, and it is certainly impossible to take part in international trade without the ability to move data across borders. While data flows are important for almost every kind of business, regardless of sector, their importance is perhaps best illustrated using the example of companies involved in – and reliant on – global value chains (GVC). In a previous study we identified five main reasons why manufacturers need to move data for their GVC production process to work:

Figure 3. Five reasons why data must be moved



Personal data makes up a large part of the data being produced and transferred for most companies, regardless of whether they are involved in a GVC. If a person wishes to participate in modern society – using digital solutions to communicate, browse, shop, share and search for information – it is impossible to do so without personal data being collected and transferred.

Table 1. Examples of personal data in production

	Personal data used	Personal data generated
Control/coordination	Employee data, user data, social media data	Employee data
Pre-production	User data, social media data	Names and CV of scientists/ researchers, test-persons' user data
Supply chain management	Customer data	Business contacts
Production	User data	Employee data
Post-sales	User data, sensor data	User data, social media data

Here customer data refers to data relating to a manufacturer's customers and their employees. User data is about how a product is used. Employee data can range from, for example, names and salaries, to how a person behaves and operates a machine.

Besides the economic importance of cross-border data flows, they are also important for the advances they have enabled in a wide range of fields. Examples include **telemedicine**, where data flows enable health professionals located in one country to monitor and even treat patients located in another country – or **environmental goods**, which often contain software components that are dependent on cross-border data flows for their continuous

operations. During the COVID-19 pandemic, **3D-printing** (a technology that relies on cross-border data flows for the transfer of design files) became an important way to produce personal protective equipment¹⁹.

It is therefore no exaggeration to say that global economic growth and, indeed, prosperity depends on how effectively regulatory regimes leverage the benefits of cross-border data flows. This highlights the importance of identifying pathways to address the challenges associated with regulations on cross-border data flows.

2.2 Regulating cross-border data flows

The regulation of cross-border personal data flows is pertinent as it requires striking a delicate balance between the huge economic importance of data and other important policy interests such as privacy, the protection of personal data, or national security. Historically, cross-border trade in services has been relatively free across many jurisdictions. But many services that previously required a physical presence or physical delivery can now be offered digitally. As a result of this ‘boom’ in digitalisation, the world has seen an incremental growth in the number of regulations governing data flows. Indeed, cross-border personal data flows are now regulated to some extent in most countries.²⁰ These regulations commonly take the form of legal requirements to store data at data centres within a country’s borders, and/or regulations that restrict the ability to move data across borders.²¹

2.2.1 The need to regulate

The different motivations behind restricting cross-border personal data flows can be summarized into three broad categories that can (and frequently do) compete with each other²²:

- Security
- Economic development
- Privacy.

To most governments, **security** issues rank amongst the most prominent concerns. They are related to one of the most basic functions of a state, i.e. to keep its citizens safe from harm (especially harm derived from foreign sources in the case of national security concerns). The arguments for not restricting data flows mainly centre around economic benefits, and these seldom trump security concerns, which makes data flow restrictions based on security concerns fairly immutable. Motivations can range from wanting to keep sensitive data out of the hands of foreign adversaries, to ensuring that domestic law enforcement agencies have access to data that can be used to investigate crimes. Cybersecurity, as a subset of security issues, is not something we focus on this

19. NBT, Advancing the Green and Digital Transition: Possibilities for an expansion of the WTO Information Technology Agreement, ITA3 (2024) and NBT, Making Green Trade Happen – Environmental Goods and Indispensable Services (2014).

20. Ferracane Martina Francesca, Hoek Bernard M., Van Der Marel Erik and Santi Filippo, Digital trade, data protection and EU adequacy decisions (2023).

21. NBT, No Transfer, No Trade, and see Chapter 2.2.2.

22. This simple categorization is intended to help our discussion, not provide an exhaustive list of the various reasons why policymakers impose restrictions on cross-border data flows. Indeed, it is not always possible to discern the *exact* reasoning behind a restriction. As an example, it is not uncommon for restrictions on cross-border data flows that are officially motivated by privacy or national security concerns to also attempt to promote domestic companies at the expense of foreign competition.

study, but we have published other reports dealing with cybersecurity from a product regulation perspective²³.

However, many developing countries (along with some developed countries) focus on concerns related to **economic development** that centre around ensuring that the economic benefits of data flows are realized in a domestic setting. From this perspective, data is viewed as a resource²⁴. As is the case with other resources, such as raw materials, governments in developing countries may wish to promote added-value processing inside the country. Thus, allowing the data to flow freely out of the country could leave developing countries locked in a lower ‘tier’ of a value chain, impeding present – and especially future – economic growth.

As we mentioned when making the case for why any recommendation needs to be realistic by taking into account that nations have different priorities²⁵, countries may also have development concerns in mind when choosing *not* to regulate cross-border personal data flows. For example, this could be the case where choosing not to impose strict restrictions to protect personal data could instead allow domestic service suppliers to create more value from the data, and avoid reducing the competitiveness of exports to third countries with less stringent data protection standards.²⁶

A number of developed countries have also raised concerns about competition policy, arguing that restrictions on cross-border personal data flows are needed to ensure that competition between foreign and domestic companies utilizing data remains (or becomes) fair. However, the underlying motivations seem to be largely the same: to ensure that the economic value of data benefits domestic consumers and businesses.

Figure 4. Reasons to regulate



Lastly, there are **privacy** concerns, possibly the main reason for regulations on the flow of personal data. We have already stated that online privacy regulations centre around diverging definitions of personal data. Many forms of online activity seem anonymous at first glance, but actually generate PID that could be used to identify an individual. This data is mostly used to show us ‘personalised’²⁷ advertising. But there are also far more serious uses, as revealed by, for example, the Facebook–Cambridge Analytica data scandal and the global mass surveillance programmes run by different governments.

23. See NBT, Innovation, AI, Technical Regulation and Trade (2023) and NBT, The Cyber Effect – the implications of IT security regulation on international trade (2018).

24. Notwithstanding the intrinsic logic of such reasoning, in many respects, data is different from raw materials. Notably, although some value might be lost, data, unlike raw materials, is not consumed when processed and could be used again for the same or for an entirely different purpose.

25. See Chapter 1.

26. Matoo and Meltzer, ‘International Data Flows and Privacy’.

27. Advertising that the advertisers *believe* is relevant to our interests.



In the EU’s approach to personal data flows regulation, online privacy and the protection of personal data are at the forefront, as reflected in the GDPR. As we have only chosen to look at options that would be compatible with the GDPR, **privacy and the protection of personal data will be a key aspect** of this study.

2.2.2 Regulatory options

Regulatory options exist on a spectrum ranging from the absence of any restrictions on cross-border personal data flows, i.e. where anyone can move personal data in and out of a country, save for technological limitations, to permissive options where transfer is possible provided the data handlers fulfil certain criteria, to strict controls and prohibitions on data flows.

Any regulation that restricts the cross-border flow of data, or makes them impossible/illegal, would be a **transfer restriction**. These restrictions range from simple transfer restrictions, for example, where only the data subject’s general consent is required, to strict **data localisation requirements** that do not allow for any transfer at all outside the jurisdiction in question.²⁸

A **data localisation requirement** forces data handlers to store data locally, meaning the data must be stored on servers located within a certain jurisdiction (i.e. a country). This would require the handler to either invest in a new local data centre or purchase the services of existing local data centres, along with related support services. This reliance on local data centres could then create new business opportunities for local firms, an aspect that ranges from being a ‘side effect’ to being the clear industrial policy aim of the regulation. In the latter scenario, the requirements might be coupled with mandates that clarify the need for a data handler to rely on domestic firms and services.

28. NBT, No Transfer, No Trade.

The requirements may encompass *all* data handled by the operator or be delimited to a subset of data, such as sensitive data (financial data, health data, etc.) or only data generated by activities within that jurisdiction.

Regulations on data localisation may be limited to the storage of data or may be coupled with additional transfer restrictions. Requirements could be in the form of a mandate to keep a *copy* of the relevant data on domestic servers, as is the case for the federal laws on personal data protection in Russia, and under such regulations the data is still movable to locations (with or without conditions) outside of the country, as long as a copy remains within the jurisdiction. Alternatively, the regulation can stipulate that the data must be stored locally and cannot be moved outside of the jurisdiction.

The formulation of data localisation requirements may be informed by a combination of the three reasons discussed in the previous chapter.

- Data localisation requirements may address the need for authorities to gain easier access to data for lawful purposes, such as preventing or solving crimes or addressing matters of national **security**. These kinds of security concerns feature prominently in the data protection legislation in e.g. China and Vietnam.²⁹
- A government that imposes the requirements may hope to promote **economic development** through the growth of domestic IT firms, or to promote investment in data centres and support services. This is arguably the case for the data protection laws in e.g. Malaysia.³⁰
- There may be concerns that personal data moved outside the country could be abused, either intentionally or as a result of weaker data privacy/protection regimes in other countries. Such concerns are at the centre of legal disputes involving the GDPR.

29. Baker McKenzie, 'Global Data Privacy and Cybersecurity Handbook', accessed 21-04-24.

30. McKinsey & Company, Localisation of data privacy regulations creates competitive opportunities (2022).

Box 2. Two very different frameworks for cross-border data flows

There are almost as many different options for regulating cross-border data flows as there are reasons why data flows might need to be restricted. The following two examples illustrate the breadth of regulatory approaches and concerns that are taken into account by lawmakers when creating a data regulation framework.

People's Republic of China

The regulatory situation concerning cross-border data flows in China is complex. There are several laws and regulations, with the three most important laws being the *Personal Information Protection Law*, the *Cybersecurity Law* and the *Data Security Law*. In addition to these three main pieces of legislation, there are many other laws, decisions, guidelines and industry regulations on both the national and the provincial level. These rules contain both *data localisation requirements* and *transfer restrictions*.

Some *data localisation requirements* are exclusive: certain data related to financial services and health care must be stored locally and cannot be moved out of, nor accessed from outside of, China. The same applies to “important data”, and data that contains geolocation information.

Other requirements are non-exclusive: if any personal data³¹ is allowed to be sent outside of China, a copy of such data must also be stored locally.

Assuming the data in question can be transferred out of China, *transfer restrictions* will still apply. As a first step (and with few exceptions), consent from the data subject is needed before any data can be *processed* (a term which includes transferring data outside of China). The data handler also needs to keep records of the data transfer, including the date and information on the recipient.

The next step depends on the size of the transfer(s), the content of the transfer(s) and the nature of the data handler. Some handlers may use *standard contract clauses* (of a standard approved by the Chinese authorities, specifically the “Cyberspace Administration of China”, which exists in both national and regional forms), signed by both the sender and the recipient and deposited with the Chinese authorities. Other data handlers must first pass a security assessment by the authorities. A passing grade does result in being pre-approved for cross-border data transfers for a period of two years, or until the conditions of the transfers change.

There are also a number of exceptions to these rules, such as the cross-border transfer of personal data being forbidden if the recipient is a judicial authority, unless prior approval is given by the Chinese authorities.

Chile

In Chile, the *Personal Data Protection Law* regulates most matters concerning personal data. Data may only be processed³² on certain grounds, such as having the data subject's prior written consent.

But assuming there are grounds for processing the data – such as prior written consent – the data can then be transferred to another country. There are no *general transfer restrictions* or *data localisation requirements*, though there are specific provisions for certain industries such as banking, that limit which entities that may be the recipients of personal data, and that such data may require local storage. These requirements make no distinction between recipients inside or outside of Chile.

31. This category includes personal data on a large number of individuals, sensitive personal data and personal data related to critical infrastructure.

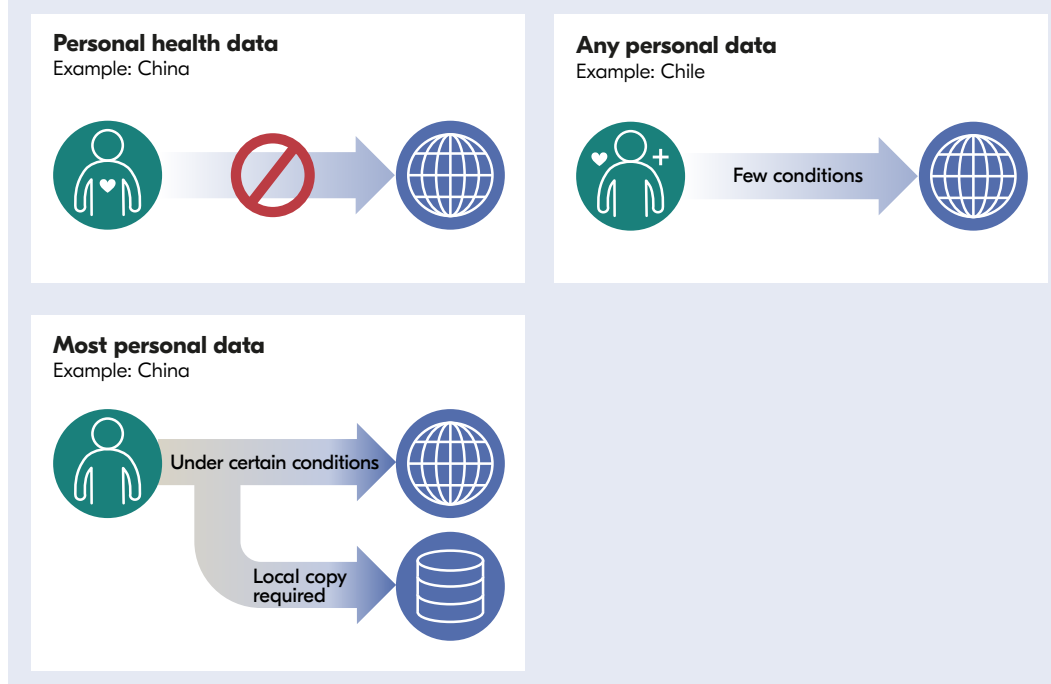
32. Like the Chinese framework, the term includes data being transferred to another country.

Box 2. continued

The data handler is required to handle the data with due diligence and is liable for any damages.

There is no specific statutory authority for personal data issues (similar to the Cyber-space Administration of China) although there are plans to create a central data protection authority.³³

Figure 5. Cross-border transfer of personal data in China and Chile



Transfer restrictions may also come without any explicit data localisation requirement. A common type of framework allows for the cross-border flow of data – even personal data – assuming certain conditions are met.

Take Brazil, for example, where legislation on data protection (the ‘General Data Protection Law’) is based on the GDPR. There are no general de jure data localisation requirements, but the transfer of personal data outside of Brazil is only allowed under certain conditions, such as when the transfer is to a jurisdiction that provides an adequate level of protection for personal data.

The situation in Brazil is typical for transfer restrictions. Where such restrictions exist, they are usually not absolute (save perhaps for certain categories of highly sensitive personal data) but are permissive, so that personal data can be transferred to a third country provided that certain conditions are fulfilled. An important distinction can be made between countries that place most of the responsibility on the data handler (“open safeguards”) and those countries where approval from the authorities is required (“pre-authorized safeguards”).

33. Baker McKenzie, ‘Global Data Privacy and Cybersecurity Handbook’, Data Guidance, ‘China: Unpacking requirements for Critical Information Infrastructure Operators’, accessed 21-04-24 and DLA Piper, ‘Data Protection laws of the world’, accessed 21-04-24.

For example, the open safeguards of the Australian Privacy Act and Privacy Principles enable data handlers to transfer personal data outside of Australia if they take reasonable steps to ensure that the recipient handles the data in accordance with the Australian Privacy Principles. Liability then remains with the data handler, the sender. Under the pre-authorized safeguards of the GDPR, however, the Commission determines to which jurisdictions a data handler may send personal data, based on the guarantee that the data will be handled according to the principles of the GDPR in that jurisdiction.³⁴

The difference in practice for a foreign company would be that if it does business in Brazil or the EU, it *might* be required to set up (or lease) separate IT infrastructure in the country, to process personal data that it cannot transfer to its HQ in a third country. While there might not be a de jure data localisation requirement, the company might de facto have to store and process certain data locally. However, the same company *will* be required to use separate IT infrastructure if it does business in China – where de jure data localisation requirements apply – while they *will not* be required to do so if they do business in Australia.

Most countries have some level of data localisation requirements, either de jure or de facto, which highlights the need to find solutions to the problems that data localisation requirements pose for businesses.³⁵

34. Baker McKenzie, '[Global Data Privacy and Cybersecurity Handbook](#)' and Australian Government – Office of the Australian Information Commissioner, '[Australian Privacy Principles](#)', accessed 21-04-24.

35. McKinsey & Company, 'Localisation of data privacy regulations creates competitive opportunities'.

3 The GDPR

The EU's General Data Protection Regulation contains both transfer restrictions and de facto localisation requirements, which limit the cross-border flow of personal data not only for businesses in the EU but also in the many countries that have based their own data protection framework on the GDPR, and for those multinational companies³⁶ that have chosen to apply the principles of the GDPR to all their operations.

This is an example of the 'Brussels Effect'³⁷, whereby the regulatory approach of the EU influences regulations and business decisions in other jurisdictions, because of the size and importance of the EU as a market.

In the EU, however, the protection of personal data goes beyond the GDPR as it is also enshrined in the Charter of Fundamental Rights of the European Union (CFR). The CFR guarantees a fundamental respect for the private life of citizens³⁸ and, more specifically, for the protection of personal data³⁹. Together with the EU Treaties, the Charter is the supreme norm of the EU, which means that any other EU rule must comply with its provisions. The general rule is that the free flow of data is subordinate to the fundamental privacy rights and, in case of conflict between the two, the privacy rights will prevail.

This puts the protection of personal data – and the GDPR – in a very strong position in the EU. It is very unlikely that the GDPR would be amended in a more permissive direction, given the political ramifications of doing so. But even *if* the requirements of the GDPR were to change, the rights guaranteed by the CFR (as interpreted by the CJEU) would continue to require restrictions on the cross-border flow of personal data, a fact that highlights the need to find recommendations for moving forward that are compatible with the GDPR.

The basic rule of the GDPR is that data handlers cannot process personal data without a legal basis. The GDPR provides an *exhaustive* list of legal bases, such as the data subject's consent to the processing of their data or if such processing pursues a legitimate interest or is necessary for the performance of a contract to which the data subject is party.⁴⁰

In addition to this are two important principles for the processing of personal data. First, personal data must be collected only for well-defined purposes, and may not be further processed for other purposes (the 'purpose limitation principle').⁴¹ Second, the collected data shall be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* (the 'data minimisation principle').⁴²

36. See, for example, Microsoft, 'Microsoft's commitment to GDPR, privacy and putting customers in control of their own data', accessed 21-04-24.

37. For more information, see the seminal *The Brussels Effect: How the European Union Rules the World* by Anu Bradford.

38. Charter of Fundamental Rights of the European Union (CFR), art. 7.

39. CFR, art. 8.

40. GDPR, art. 6.

41. GDPR, art. 5(1)(b).

42. GDPR, art. 5(1)(c).

These requirements collectively limit the ability of EU businesses to transfer personal data across borders⁴³. Such transfers are deemed particularly sensitive insofar as the level of data protection in third countries is lower than in the EU⁴⁴. Thus, while the GDPR does not mandate de jure data localisation (only transfer restrictions), the requirements for cross-border transfers of personal data are so stringent that the situation can be characterized as a de facto data localisation requirement.⁴⁵

3.1 Cross-border data flows per the GDPR

The GDPR allows the transfer of personal data to third countries in three situations only.

- 1) The transfer of personal data to those countries that ensure an **‘adequate level of [data] protection’** is permitted without restrictions.⁴⁶ It is for the EU Commission to approve those countries by way of a so-called ‘adequacy decision’. Approval is granted following an investigation by the Commission of the country’s relevant legislation on data protection and, more generally, the respect of human rights and fundamental freedoms, as well as on the existence of independent supervisory authorities and of effective remedies provided to data subjects if their rights are breached. To date, only slightly more than a dozen countries (ranging from Argentina to Japan) have been issued adequacy decisions.
- 2) Businesses may transfer personal data to third countries if they have provided **‘appropriate safeguards’** to protect the rights of data subjects.⁴⁷ The GDPR introduces several such safeguards, the two main ones being Binding Corporate Rules (BCR) in the case of data transfer between businesses belonging to the same group, and Standard Contractual Clauses (SCC) in other situations. Both BCRs and SCCs are essentially legal agreements between businesses that regulate the transfer of data outside the EU. Depending on the situation, they may need to be approved by the Commission or a national data protection authority of a Member State.
- 3) In the absence of an adequacy decision or other appropriate safeguards, the transfer of personal data to a third country may be permitted in **specific circumstances** defined in the GDPR.⁴⁸ Such transfers are additionally subject to strict conditions, for example, the informed and explicit consent of the data subject, the existence of a public interest, or the need to perform a contract concluded in the interest of the data subject. Given the limited nature of these specific circumstances, this third option for cross-border data transfers is not useful for the day-to-day operations of businesses.

43. In the case of the GDPR, the “border” is the whole of the EU and not a single EU member state.

44. Obviously, the safeguards of the GDPR could, in practice, easily be circumvented if personal data were processed in countries lacking adequate protections.

45. UN Trade and Development (UNCTAD), Digital Economy Report 2021 – Cross-border data flows and development: For whom the data flow (2021) and Chander Anupam, ‘Is Data Localisation a Solution for Schrems II?’, *Journal of International Economic Law* (2020).

46. GDPR, art. 45.

47. GDPR, art. 46 and 47.

48. GDPR, art. 49.



3.2 The GDPR test

The GDPR restrictions on cross-border personal data flows severely limit the kind of recommendations that could be considered to mitigate the global challenges that businesses face with cross-border data flows. Any recommendations need to take into account several red lines.

As a general principle, the level of protection of personal data in the EU is not negotiable. Thus, it cannot be lowered or otherwise circumvented by means of, for example, a free trade agreement or some other international instrument. This does not mean that there are no bilateral or multilateral solutions that could facilitate the flow of personal data, only that they cannot result in a lowering of the standards for personal data protection in the EU.

There must be guarantees that the level of protection will not be lowered, and it is not sufficient that any third country offers such guarantees in writing. Experience from the case law of the CJEU points to the need to demonstrate the existence of effective and enforceable legal mechanisms that limit the authorities of that country and offer remedies in case of breaches of the rights of data subjects.

A particularly sensitive point to be considered here is the possible use by authorities in third countries of personal data for public or national security reasons. Any third country laws that give authorities access to personal data for the purpose of public or national security must be clear, precise and proportionate. In other words, generalised processing of personal data for national security purposes is not allowed and, in practice, the GDPR requires that EU law protecting personal data has primacy over third country laws that aim to safeguard national security.⁴⁹

The CJEU's judgement in Schrems II shows that this applies not only to adequacy decisions, but also to the use of SCCs. A company using SCCs to transfer personal data

49. Schrems I and Schrems II.

outside of the EU cannot rely on contracts alone, it must also verify that the protection offered to the personal data of EU subjects is up to the level required in the GDPR.

Regardless of the measures adopted to facilitate cross-border data flows, the EU would have to retain a unilateral right to ensure that this is done in line with EU constitutional rights set in the CFR. If an instrument (such as a free trade agreement) proves insufficient to protect the rights of data subjects, the EU may, under EU law, take any appropriate measures to remedy the situation. This could include a unilateral withdrawal from that instrument or imposing additional conditions for its application.

Box 3. Is the recommendation compliant with the GDPR?

If there is a mechanism that allows for personal data to be transferred to third countries, then:

- The level of protection of personal data must be essentially equivalent to EU/GDPR standards and may not be lowered.
- The level of protection must be guaranteed by effective enforcement mechanisms.
- The EU must retain the unilateral right to change or withdraw from agreements.

4 Challenges

Previously, we have described the importance of cross-border data flows and why they are often regulated. In this chapter we identify and describe the problems and challenges facing businesses, as a result of such regulations. We begin with the GDPR, before moving on to a more general global look at the challenges facing businesses.

4.1 The challenge of complying with the GDPR

As we mentioned in Chapter 1, for a recommendation to be viable it should not be limited to a ‘one-size-fits-all’ approach. Achieving a good balance between different, and sometimes conflicting, data-related concerns through the regulation of cross-border personal data flows might look very different in Austria compared to Ghana.

The GDPR is the result of circumstances within – and the balance sought by – the EU. The regulatory approach chosen by the EU puts the protection of personal data and privacy rights above the free flow of data, and the associated economic benefits. Political support for this approach is high⁵⁰, but the GDPR does create a number of challenges for businesses.

Costly

The most obvious problem is the direct costs associated with the GDPR. Ahead of the GDPR entering into force, the 500 largest companies in the world were expected to spend a total of almost USD 8 billion to ensure compliance, while medium-sized companies would have to spend, on average, half a million dollars each.⁵¹ A report that looked at the costs of the GDPR shortly after it entered into force revealed that some companies were required to spend over EUR 10 million annually on GDPR compliance alone.⁵²

More recent studies have found similar results. Developing the necessary processes, hiring the necessary staff and having the required IT infrastructure to comply with the GDPR entail costs. One study estimates that, on average, businesses in the EU experienced an 8 per cent reduction in profits along with a 2 per cent decrease in sales as a result of complying with the GDPR. The GDPR reduced the volume of web traffic for the travel industry, reduced data sharing online, increased market concentration among (mostly American) web technology vendors⁵³, and had a negative effect on capital investments in tech companies in the EU.⁵⁴

It might be easy to imagine that these effects are primarily a problem for large, US-based tech companies with plenty of cash at hand. However, the effects have been more severe for smaller tech companies, which have seen double the average decline in sales due to the GDPR.⁵⁵

50. Noyb, ‘5 Years of the GDPR: National Authorities let down European Legislator’, accessed 21-04-24.

51. Financial Times, ‘Companies face high cost to meet new EU data protection rules’, accessed 21-04-24.

52. Chen Chinchih, Benedikt Frey Carl, Presidente Giorgio, Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally (2022).

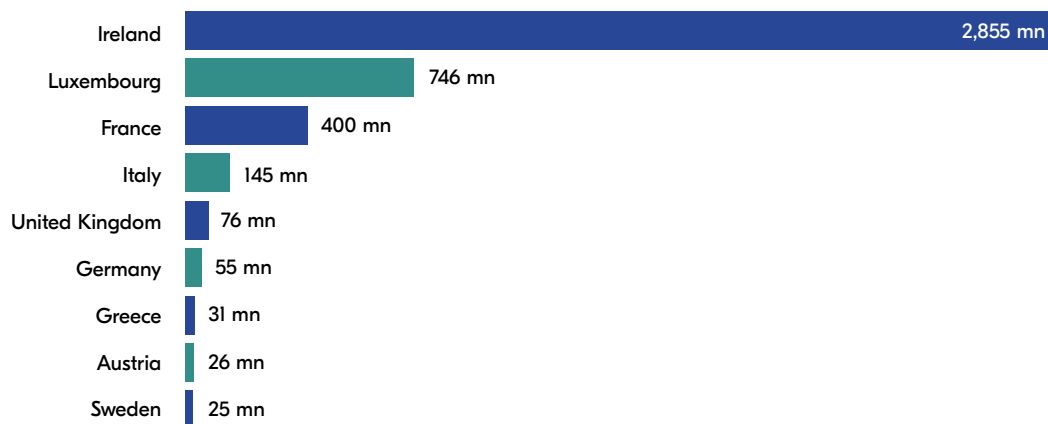
53. Geradin Damien, Karanikioti Theano, Katsifis Dimitrios, ‘GDPR Myopia: how a well-intended regulation ended up favouring large online platforms – the case of ad tech’, European Competition Journal, vol. 17 (2021).

54. Chen, Benedikt, Presidente, Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally.

55. Ibid.

The same is true for those companies that have not complied with the GDPR, the penalties for which can be quite severe, regularly running into millions of dollars. The largest fines have already passed the USD one billion mark. However, out of the more than 1000 penalties that have been issued since the GDPR came into force, the majority have been cases involving SMEs.⁵⁶

Figure 6. Highest GDPR fines by country in EUR⁵⁷



Inflexible

A more serious problem, however, is the relative inflexibility of the GDPR. As mentioned in Chapter 3, the kind of free flow of data across borders that could more fully materialize the benefits of digitalisation is only possible between the EU and other countries that have been deemed to have an adequate level of data privacy protection. As the Schrems I and Schrems II cases show, the CJEU’s interpretation of ‘adequate’ puts the term very close to ‘equivalent’.

This effectively means that it is very difficult to establish the free flow of data between the EU and any country that has a different view on how security, economic development and privacy concerns should be balanced.

SCCs and BCRs are limited in functionality

A partial remedy to the problem of inflexibility can be found in SCCs and BCRs (see Chapter 3), which are designed to allow data to flow between the EU and third countries in the absence of an adequacy decision.

However, the actual functionality of these personal data transfer mechanisms is limited, and the CJEU has ruled that the same high level of protection of personal data that is required for an adequacy decision is, essentially, also a requirement for the use of SCCs⁵⁸.

SCCs are also difficult to use, as they need to be designed to deal ex post with all possible data transfers. If the scope of the data processing changes, new SCCs must be drafted and implemented, making for an inflexible data transfer mechanism.

56. IT Governance, ‘[How Much Does GDPR Compliance Cost in 2023?](#)’, accessed 21-04-24 and EQS Group, ‘[The Biggest GDPR Fines of 2023](#)’, accessed 21-04-24.

57. EQS Group, ‘[The Biggest GDPR Fines of 2023](#)’.

58. See Chapter 3.

BCRs, which only apply to intra-company data transfers, instead require a lengthy process of implementation and approval.

For either mechanism, a company may require specialists with knowledge of data mapping, as well as auditing services, meaning neither option is very attractive for SMEs with limited resources to deal with complex legal and technical issues.⁵⁹

Adequacy decisions are only a partial solution

Adequacy decisions represent one way forward that – once implemented – allow for the free cross-border flow of personal data. However, an adequacy decision is really only possible for countries that either view the balance between data-related concerns in a very similar way to the EU, or are willing to adopt a GDPR-like data protection regime regardless.

Adapting such rules requires extensive commitments, including creating data protection authorities and offering EU citizens who believe their personal data has been mishandled the adequate legal and administrative recourse. Neither is an adequacy decision necessarily permanent, as ensuring a level of data protection that is ‘essentially equivalent’ to the EU requires periodic reviews. If the level of data protection is found to be inadequate, any adequacy decision may have to be rescinded.

This goes some way towards explaining the limited number of adequacy decisions that have been made so far. The first agreement, the ‘Safe Harbor agreement’ with the US, predates the GDPR and was signed in 2000⁶⁰. Since then, the EU Commission has issued an adequacy decision to 14 different jurisdictions, including the most recent iteration of contested agreements with the US. If you exclude territories that are European microstates already closely aligned with the EU, member states of the EEA or overseas dependencies of current or former (UK) EU member states, and that number drops to eight, out of the hundreds of global jurisdictions.⁶¹

Using a broad definition of ‘free trade agreement’, the EU has concluded five times as many free trade agreements during the same period. Progress on adequacy decisions must therefore be characterised as slow.

Unlike free trade agreements, an adequacy decision is a unilateral decision, though it does establish a ‘bilateral’ area of free data flows. However, the fact that the EU has granted an adequacy decision to both Japan and Uruguay does not necessarily mean that data can flow freely between these two countries. It should, however, make any bilateral or unilateral agreement between two such countries significantly easier.

Research indicates that an adequacy decision leads to an increase in digital trade between the EU and the third country. Adequacy decisions also lead to greater digital trade between countries to which the EU has granted an adequacy decision.⁶²

59. Matoo and Meltzer, *International Data Flows and Privacy* and Ferracane, Hoek, Van Der Marel, Santi, *Digital trade, data protection and EU adequacy decisions*.

60. The GDPR is based on previous EU data protection legislation, such as the Data Protection Directive.

61. EU Commission, *‘Adequacy decisions’*, accessed 10-11-24.

62. Kuner Christopher, *‘Reality and Illusion in EU Data Transfer Regulation Post Schrems’*, *German Law Journal* (2017).

4.2 A global patchwork problem

Although it is central to this study, the GDPR is still only one of many regulatory frameworks for governing cross-border data flows. Counting just the member states of the G20, new data governance regulations were proposed virtually every day in 2023, and more than 1900 new regulations have been proposed since 2020.⁶³

Businesses normally find uncertainty in regulatory environments to be unfavourable and, conversely, they are usually in favour of transparent, predictable and stable regulatory environments. Unfortunately, the regulatory situation for cross-border data flows is anything but. Major markets such as the EU, China and the US are taking very different approaches to how cross-border data flows should be regulated.

This not only complicates and raises the cost for businesses of operating in multiple markets but it also hinders internationalization and growth, impacting competitiveness.⁶⁴

In a study from Japan from 2022, a number of companies – whose business models rely on cross-border personal data flows – were interviewed about the challenges they face due to regulatory fragmentation and lack of transparency. They reported the following:⁶⁵

- Difficulties in determining what kind of activity can be classified as a cross-border flow of data, and thus be subject to regulations on cross-border data flows. As an example, one of the companies stated it was unsure whether the definition would include personnel on a business trip to a third country accessing company servers located in their home jurisdiction.
- When a business receives data from another company located in a third country, it may be required to comply with contractually stipulated data origin laws. The process required can be very complex, and added to that complexity is the issue of language barriers. There might be limited availability of information about these laws in the native language of the receiving business, or in the *lingua franca* of the internet, English⁶⁶. Laws and regulations are also often constructed in such a way that other documentation, such as guidelines or recommendations, is required to fully grasp the meaning of any rules, further compounding problems with language barriers. For many businesses, having a separate legal team in place in every country where they do business is not financially feasible.
- The application of laws and regulations on cross-border data flows often boil down to the meaning of crucial terms such as “adequate”, “safe” or “sufficient”, especially concerning the transfer of personal data. However, the meaning of such terms may differ greatly between different jurisdictions, making it difficult for businesses to plan or requiring them to err on the (costlier) side of caution. Some definitions are open to interpretation, while the penalties for using the wrong interpretation can be costly.
- Even within the same jurisdiction, regulatory authority concerning data flows can be scattered across multiple agencies. This often precludes the holistic understanding favoured from a business perspective, resulting in regulatory duplication and confusing rules.

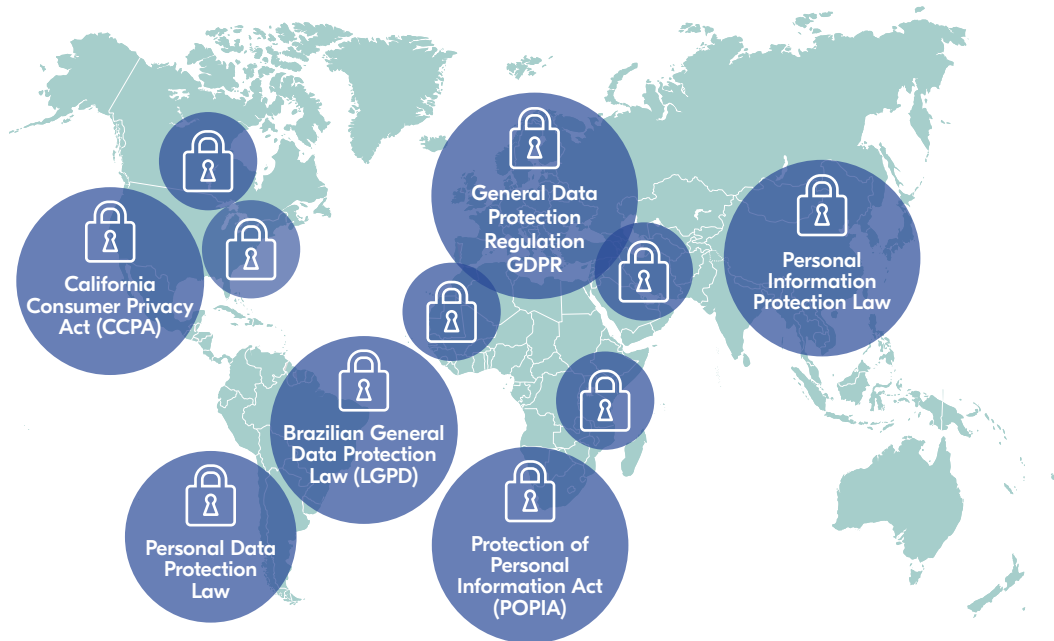
63. WEF, From Fragmentation to Coordination and Digital Policy Alert, ‘[Activity Tracker](#)’, accessed 05-02-23.

64. Casalini Francesca, González López Javier and Nemoto Taku (OECD), Mapping commonalities in regulatory approaches to cross-border data transfers (2021).

65. Ministry of Economy, Trade and Industry (Japan), Interim Report of the Expert Group on Data Free Flow with Trust (2022).

66. New York Times, ‘How the English Language Conquered the World’, 2022.

Figure 7. Regulatory patchwork



Navigating such difficulties is a challenge for any business but is especially difficult for SMEs, which lack the resources of larger multi-national businesses. Another report, also based on global surveys, highlights the challenging situation for SMEs in particular: based on the feedback, the single most critical issue for SMEs is the lack of legal transparency that springs from regulatory fragmentation.⁶⁷

A third study of businesses in the signatory countries of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership found that barriers related to personal data flows, such as privacy and local storage requirements, were some of the greatest challenges facing online exporters.⁶⁸

Businesses also face issues in balancing data protection legislation with other regulatory requirements, such as the balance between the rules on preventing money laundering and the rules protecting personal data.⁶⁹

4.3 Economic inefficiencies

Barriers to trade often result in economic inefficiencies, i.e. resources being utilized in a less-than-optimal manner, and the same is true for restrictions on cross-border personal data flows.

Such inefficiencies constitute one of the most serious negative effect stemming from these restrictions. The case of cross-border personal data flows and global value chains illustrates this well.

67. WEF, *From Fragmentation to Coordination* and Suominen Kati, *The CPTPP's Impacts on Digital Trade and the Path Forward* (2021).

68. *Ibid.*

69. WEF, *From Fragmentation to Coordination*.

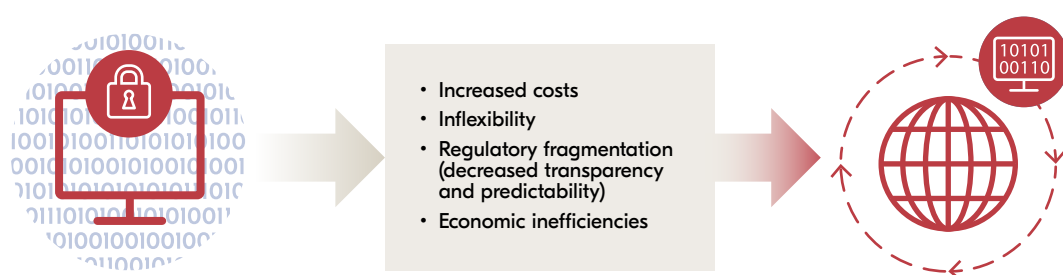
In a previous report we analysed the effects of restrictions on cross-border personal data flows in global value chains and found two prominent effects: 1) changes in how GVCs are set up and 2) less optimal functioning of the GVC. As the changes in how GVCs are set up usually come in the form of less optimal operations, the two go hand in hand.

Data localisation requirements can impact how a **GVC is set up**. Businesses may be required to move part of their operations to a country with data localisation requirements in order to do business there at all. One company interviewed for our previous study explained how they were required to move part of their post-sales operations to a country with data localisation requirements. They were also unable to move data produced by their products and users in that country out of the country, meaning they could not offer online repair solutions, remote monitoring or rely on expertise provided from abroad.⁷⁰

When businesses involved in GVCs are unable to move data freely across borders or are required to store data locally, they may need to use multiple ICT systems, systems which, in turn, might not be able to seamlessly communicate with each other. Running multiple systems usually comes at an increased cost and runs contrary to the general ambition of companies to streamline their processes to increase efficiency and synergies, instead resulting in **GVCs functioning less than optimally**. Streamlining is often necessary for a company's competitiveness, and the impact of regulations on data flows can be significant, especially if this means a company is required to have both data and personnel on location in every (or at least most) markets. Reducing the ability of a business to streamline may also undermine the possibility of consolidating operations globally and reaching scale, which ultimately may reduce the competitiveness of the national economy.

Additionally, restrictions on cross-border data flows can negatively impact the ability to control and coordinate a GVC. This is especially true for business models that rely on being able to instantly and seamlessly move information on inventories, package locations and similar data to coordinate just-in-time delivery and lean production methods.⁷¹

Figure 8. The cost of compliance



70. NBT, No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods (2015).

71. NBT, No Transfer, No Production.

4.4 The cost of technological advancements

Digitalisation is virtually synonymous with technological advancements, and cross-border data flows are a crucial part of everything from training new artificial intelligence (AI) models to utilizing blockchain technology.

For innovators active in the EU, the GDPR has the effect of slowing down technological advancements. As an example: developing AI models requires huge data sets, something that is difficult to reconcile with the GDPR, as the GDPR mandates *minimizing* the amount of data collected on individuals.⁷² The EU is already lagging far behind other major economies – the US and China – when it comes to the development and utilization of new technologies such as AI.⁷³

Restrictions on cross-border personal data flows, in the EU as well as in other markets across the globe, risk hampering innovation and technological advancements across a wide range of sectors, including traditional manufacturing. These negative effects are more severe for SMEs than for larger companies.⁷⁴

It is important, however, to also mention something about the environmental impact of these developments. Progress is not without cost.

Data *flows* into and out of hardware systems, systems that require electricity. Rapid developments in fields such as AI will greatly increase the amount of electricity required. In the US, for example, data centres (through which nearly all internet traffic flows⁷⁵) accounted for 4 per cent of total national electricity consumption in 2022, but projections show that this figure will increase by 50 per cent in just a few years (to 2026). In 2011, Google estimated that the electricity required to power a single search query was the equivalent of powering a 60W lightbulb for 17 seconds. However, a query by modern AI-powered systems like ChatGPT already use 15 times more electricity than this.⁷⁶

This increase in demand is happening as the electrification of heating infrastructure and transportation systems is already putting a serious strain on both national and local energy grids around the world.⁷⁷ At the same time, there are estimates that 90 per cent of the data generated by people, products and businesses is never used again after it is first stored, or after a couple of months in storage.⁷⁸

Although these sustainability concerns are not solely related to cross-border data flows, but to the broader digital transition, data flows still form an integral part of digitalisation, and thus raise serious questions from a sustainability point of view. Even at the current rapid pace at which emission-free energy sources like renewables are expanding, the large amounts of electricity required by the digital transition are already resulting in significant greenhouse gas emissions and will likely continue to do so in the near future. Added to this is the use of water (for cooling systems in data centres and for producing electricity) and land (for data centres).⁷⁹

72. Congressional Research Service, *Data Flows, Online Privacy and Trade Policy* and Thierer Adam, 'Artificial Intelligence Primer: Definitions, Benefits & Policy Challenges', accessed 10-11-24.

73. Thierer Adam, *GDPR & European Innovation Culture: What the Evidence Shows*, accessed 10-11-24.

74. NBT, No Transfer, No Trade.

75. Deutsche Welle, 'Data centers keep energy use steady despite big growth' (2022).

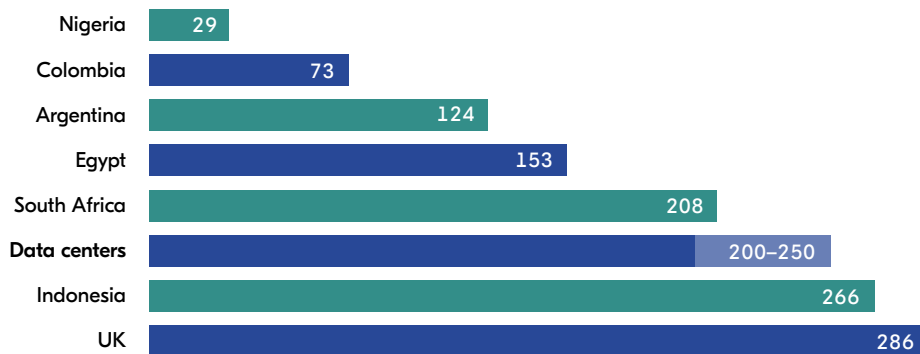
76. Leffer Lauren, 'The AI Boom Could Use a Shocking Amount of Electricity', *Scientific American* (2023).

77. New York Times, 'Google Details, and Defends, Its Use of Electricity' (2011).

78. McGovern Gerry, *World Wide Waste: How digital is killing our planet – And what we can do about it*, (2020).

79. Al Kez Dizar, M. Foley Aoife, Laverty David, Furszyfer Del Rio Dylan, and Sovacool Benjamin, 'Exploring the sustainability challenges facing digitalisation and internet data centers', *Journal of Cleaner Production*, vol. 371 (2022).

Figure 9. Data centre electricity usage.⁸⁰ Domestic electricity consumption vs. data centres in 2020 in TWh.



Some restrictions on cross-border personal data flows, such as data localisation requirements, exacerbate the situation by increasing the environmental impact. A company required to operate several data centres in multiple countries instead of a single centre in a single country would very likely use more electricity, water and land, although usage would depend on local conditions.

However, even if all data localisation requirements were to disappear in the near future, it would be difficult to discuss the digital transition, and with it, cross-border data flows, without also broaching the subject of the environmental impact. Although we offer no recommendations on how to best balance these issues, it is important to note that measures to benefit more from digitalisation by facilitating the free flow of data may, without any intervention, lead to an increase in the environmental impact of digitalisation.

80. Deutsche Welle, 'Data centers keep energy use steady despite big growth'.

5 Recommendations

Personal data can be many things: a ‘raw material’-like resource, a component of the right to privacy, a national security issue, or all of these at the same time and more. The economic value aspect of cross-border data flows in particular bears repeating; they are expected to form the basis for the future growth of the global economy.

Policymakers dealing with digital trade must weigh the many different aspects of data flows – including the economic benefits – against each other. To meet important development, security and/or privacy goals, governments across the globe have seen the need to regulate if, and in what way, personal data may be moved to other countries.

The regulatory situation, however, poses numerous challenges for businesses and (by extension) for society at large, such as increased costs and economic inefficiencies. Notwithstanding these negative effects on a crucial component of modern production and international trade, regulatory frameworks such as the GDPR – which restrict the cross-border flow of personal data – are here to stay and, if anything, become more prevalent in the future.

Thus, the challenge for policymakers, as well as the purpose of this study, is to find pathways forward – what we call **recommendations** – that can mitigate the problems arising from the regulatory situation for cross-border data flows.

5.1 Convergence around a common terminology

It is unlikely that we will reach an international consensus on the level of protection of, for example, personal data, given that countries have such disparate views on the balance between privacy, development and security concerns.

It might, however, be possible to reach a common understanding of *what* personal data is. Countries interested in facilitating the cross-border flow of data could standardise the meaning of common and operationally important terms such as ‘personal data’, ‘metadata’, ‘cross-border transfer’ or even ‘adequate level of protection’, as they relate to the rules governing cross-border data flows. Progress on harmonisation has already been made, in initiatives like the previously mentioned APEC Cross-Border Privacy Rules, as well as in the form of international trade agreements that include rules on cross-border data flows (and therefore, by necessity, some common definitions). Additionally, the OECD Privacy Guidelines provide some common definitions.⁸¹

A point of departure could be to take advantage of the work that has already been done in these forums on developing a common terminology, by separating that work from discussions that also deal with the significantly more difficult and contentious issue of regulatory harmonisation. Standardised definitions could then be codified separately in an international instrument, such as a joint declaration, a trade agreement or a separate agreement on digital issues. The way that the UN model laws are used could be a source of inspiration.

Standardising common terms would go some way towards mitigating the patchwork problem. A company doing business in Australia, Chile and the EU would still need to adapt to three different frameworks for transferring personal data between these countries, but it would only need to contend with one meaning of terms such as ‘transfer’ or

81. (OECD) Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

‘personal data’. Although a patchwork would remain, it would be easier to navigate. A clear and widely used definition of *personal data* could be particularly beneficial to businesses, by allowing them to separate and transfer non-personal data (the transfer of which, as mentioned, is subject to far fewer restrictions) across multiple jurisdictions. Such a solution would also directly address requests from businesses to simplify regulations.⁸²

Countries participating in such an initiative would not be required to change the level of protection of personal data. To the extent that changes would be needed in existing legislation, the level of protection could be designed to remain the same but with different terms (or different meanings of the same terms).

There could be an advantage to starting with a smaller group of countries at first and then expanding, as well as engaging in a public-private dialogue (that includes both data protection and trade policy authorities) to agree on common definitions. A disadvantage, however, would be that any changes would add to the already rapid pace of changes in the data protection regulations.

Useful, realistic and GDPR-compliant?

Standardising terminology would be **useful** for addressing regulatory fragmentation and also **realistic**, as the focus would be on harmonizing terminology rather than rules. No changes to how the regulations restrict cross-border data flows would be required, but a common terminology would still be easier for businesses to contend with.

It would also be **compatible with the GDPR** as it would not result in any reduction (or change at all) in the level of protection of personal data. The EU has not been able to participate in the many ongoing initiatives on regulatory harmonisation due to the restrictions of the GDPR, but the block would be able to participate in an initiative to harmonise terminology.

Implementation might require changes to the GDPR, but as long as the level of protection is left unchallenged, EU privacy law does not need to be immutable.

5.2 More, and faster, adequacy decisions

The EU Commission could be encouraged – or even required – to initiate more adequacy investigations, and measures could be taken to improve the process, making for faster investigations.

While it is solely at the discretion of the Commission to approve (or reject) the data protection regimes of third countries as adequate, there is nothing to prevent the introduction of a recommendation or an obligation for the Commission to initiate the investigation that precedes an adequacy decision.

A natural venue would be a free trade agreement between the EU and another party, and the possibility of initiating an adequacy investigation could then be seen as something that improves the EU’s ‘offer’ in trade negotiations. It would be up to the EU member states to introduce a recommendation – or an obligation – to initiate an adequacy investigation as part of the mandate given to the EU Commission to negotiate a free trade agreement. An obligation could also be more detailed by including items such as a timeline. To facilitate the investigation and as part of the negotiations for a trade

82. Ministry of Economy, Trade and Industry (Japan), Interim Report of the Expert Group on Data Free Flow with Trust.

agreement, obligations could also be placed on the partner country to cooperate by ensuring access to information or documentation necessary for the investigation. To avoid resources being wasted, exceptions could be included that would allow the Commission to end any investigation prematurely if, for example, preliminary findings indicate that important aspects of the data regulation framework in the partner country are clearly incompatible with the GDPR.

A secondary (and complementary) option would be to simply increase transparency around the adequacy decision process. Adequacy decisions are made on a case-by-case basis, but the Commission uses internal guidelines for evaluating the data protection framework of third countries.⁸³ These guidelines could be made public and easily accessible, as could documentation on the processes behind existing adequacy decisions.

This would benefit countries interested in being considered adequate for data protection purposes. Long before any formal – or even informal – process with the Commission is launched, these countries would be able to better evaluate the advantages and disadvantages of the reforms that would be required for an adequacy decision. They could also begin working on these reforms.

Business and civil society groups in other countries would also gain a better understanding of the requirements for adequacy decisions, which would be useful in their dialogue with government actors, especially when such groups are pushing for changes to existing legislation.

Transparency and ease of access would be especially beneficial to small developing countries and the least developed countries, which may not be able to prioritise hiring the expertise needed to help them understand the EU's view on data regulation.

While there might be confidentiality concerns in making internal Commission documents public, such concerns could feasibly be addressed in the process of making the documents public and should in any case be weighed against the interest of increasing the number of adequacy decisions.

Adequacy decisions for third countries continue to be promoted by the Commission as the main pathway for ensuring the (mostly) free flow of data internationally, while ensuring a high standard of protection for personal data. As detailed in Chapter 3 however, there are a few drawbacks with the system, and reaching an adequacy decision is a resource-intensive process that can take years⁸⁴. Setbacks might further prolong the process, as clearly illustrated by the repeated attempts to reach an adequacy decision for the US.

Despite these drawbacks, adequacy decisions are likely to remain one of the main solutions for ensuring the free flow of data. Facilitating more adequacy decisions would thus mitigate both the patchwork problem and the cost of compliance.

83. Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems'.

84. *Ibid.*

Useful, realistic and GDPR-compliant?

This recommendation would be **useful**, but its utility would depend on the outcome of any adequacy investigations. If an adequacy decision is granted, it would greatly facilitate cross-border data flows between the EU and the partner country. It is also **realistic**, as transparency measures could be implemented without altering the adequacy criteria, though it might require EU member states to advocate for and encourage the Commission to adopt such changes. Importantly, increasing transparency would make it easier for countries to determine for themselves whether 'adequacy' is something desirable or not, without pressurizing them to change their regulatory approach.

Naturally, the recommendation is **GDPR compliant**, as it aligns with existing mechanisms and criteria for adequacy.

5.3 Technical assistance and capacity-building

Technical assistance and capacity building projects by developed countries and international organizations could play a role in promoting the cross-border flow of personal data by ensuring that a lack of resources and knowledge does not become a barrier for countries that wish to develop their data protection frameworks.

For governments that have decided that a comprehensive and stringent framework similar to the GDPR is in line with their priorities and needs regarding data protection, the process for developing such a framework may require both significant resources and know-how. This challenge can be alleviated by technical assistance.

While there are some existing (both private and public) initiatives on capacity building for data protection authorities, it appears to be an underdeveloped area in the trade policy 'aid-for-trade' context and could to a much larger extent be included as both part of negotiations on free trade agreements and as part of negotiations in the WTO^{85,86}. As an example: while it is positive that commitments on technical assistance and capacity building are included in the proposed WTO Agreement on Electronic Commerce, the commitments would be mostly non-binding and vague.

Providing functional and specific technical assistance for capacity building related to data regulation should be especially important for the EU, which is clearly invested in spreading the regulatory approach of the GDPR by way of the Brussels Effect and through negotiated efforts in trade agreements.

Many countries that may be interested in allowing a free flow of data with the EU will find it difficult to develop the necessary frameworks and institutions to safeguard personal data at the level required by the GDPR. While developing countries must be free to choose the regulatory options that best suit their needs, if a country does decide to move towards adopting a framework similar to the GDPR, this is something that the EU should not only welcome and encourage, but actively support. The resulting regulatory harmonisation would mitigate both the patchwork problem and the cost of compliance by creating a larger geographical area in which businesses only need to follow one set of rules.

85. See our previous publication NBT, The E-Commerce Negotiations in the WTO – understanding non-participation (2023).

86. WEF, Data Free Flow with Trust.

Useful, realistic and GDPR-compliant?

This approach is **useful**, as helping countries to adopt an already established regulatory approach, whether the GDPR or something else, would likely facilitate the cross-border flow of data between countries that share that same approach. As there are already existing capacity building programmes that could be expanded, it is also **realistic**.

It is fully **GDPR compliant**, as it does not introduce new mechanisms for data transfer but supports the development of compatible regulatory frameworks. Additionally, while helping countries to adopt legislation similar to the GDPR will not automatically result in an adequacy decision, it should greatly facilitate the process.

If a country adopts legislation that is similar to an established framework but which is not in line with the GDPR, this would likely complicate future efforts to establish the free flow of data with the EU. From an EU perspective, it would then be better to only support initiatives to develop regulatory frameworks that are similar to – or at least in the same direction as – the GDPR.

5.4 A ‘Data Flows Test’

An option that we previously advocated is to introduce a ‘Data Flows Test’ for regulations in the EU.

With such a test in place, legislators and regulators in the EU would be required to take into account the facilitation of cross-border data flows when either applying existing rules that restrict such flows, or when developing new restrictions. This would cover both the adoption of new adequacy decisions and the approval of new BCRs or SCCs, as well as opinions on the interpretation of the GDPR by the European Data Protection Board.

The introduction of a Data Flows Test could be achieved by applying the well-established EU law principle of *proportionality*. Before any new data flow restrictions are formulated, or when existing restrictions are applied or updated, an assessment would need to be made to establish whether there are alternative and less restrictive measures that could achieve the desired level of protection of personal data. The obligation to perform an assessment should apply at both the Union level and at the national level in EU member states (e.g. to measures adopted by the national data protection authorities). Wherever possible, the assessment (likely to be in the form of an impact assessment document) should be made public.

To ensure that the Data Flows Test is binding on the EU and national institutions, it would have to be adopted in the form of an EU legislative act. This would preferably be in the form of an EU regulation that is directly applicable in the member states and can also be addressed to all EU institutions, bodies, offices and agencies.⁸⁷ An added advantage of codifying the Data Flows Test into law would be enabling businesses to legally challenge data protection decisions that are disproportionate, i.e. put pressure on the EU to avoid legislation or regulations where the official reason is to protect privacy, but the actual goal is something else, such as industrial policy.

As an alternative, the Data Flows Test could be set in a non-binding EU act, such as a Commission recommendation. Recommendations are not binding per se but, to the

87. Similar to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, NBT, A Data Flows Test for the Single Market (2023).

extent that the Data Flows Test would codify the EU law principle of proportionality, it would – indirectly – have some legal effect. National institutions would, however, not be legally bound by such a recommendation.

The exact specifications of the Data Flow Test should be worked out by a group that includes representatives of data protection agencies, experts on privacy rights, businesses representatives and other stakeholders. As a starting point, in an earlier paper on the Data Flows Test, we proposed two options for how a test might look in practice:

- One option would be to use a generalised obligation, such as a requirement “to assess whether less restrictive means on the free flow of data could achieve an equivalent level of data protection”. Although abstract, such a formulation would be flexible enough to accommodate situations that are not foreseeable at the time of adoption. An example of such a minimalist approach can be found in the proportionality test set out in the Services Directive.⁸⁸
- A second option would be to use a checklist of detailed questions to be considered by policymakers dealing with digital trade, including the likely impact of any restrictive measure on innovation and competitiveness, the ability of businesses to adjust to the measure and an assessment of concrete alternative measures. This option would be more in line with the impact assessments that are usually conducted when EU legislation is drafted.⁸⁹

Both options could be supplemented by procedural requirements to guarantee a correct and thorough impact assessment. These could include obligations for decision-makers to: (i) collect and document evidence (including hearings with experts and other stakeholders), (ii) motivate and publish their choice for a specific regulatory option, and (iii) subject their findings to independent scrutiny.

Useful, realistic and GDPR-compliant?

This recommendation is moderately **useful**, as it primarily acts as a safeguard against increasing fragmentation, rather than addressing existing fragmentation. It is, however, **realistic** for the EU and could inspire similar measures in other jurisdictions.

The approach is fully **GDPR compliant**, as any application of a Data Flows Test would still be interpreted in the light of the CJEU rulings on the protection of personal data in the EU.

88. Article 16(1)(c) of Directive (2006/123/EC) on services in the internal market states that any requirement on services imposed by the Member States “must be suitable for attaining the objective pursued, and must not go beyond what is necessary to attain that objective.”

89. Similar to the work of the Regulatory Scrutiny Board with respect to the policy initiatives of the European Commission.

5.5 Transparency of regulations

All our previous recommendations envision the global regulatory patchwork remaining to some extent, which highlights the need to increase transparency around the regulations that will continue to make up this patchwork.

As transparency is a key issue in trade policy, several sources of inspiration are available⁹⁰.

The commitments found in the WTO Trade Facilitation Agreement (TFA) on the publication and availability of information is one such source of inspiration⁹¹. Similar commitments on data flows could be negotiated between interested countries as a solution to some of the issues arising from the patchwork problem, such as the limited availability of information on data regulations.⁹² Any such commitments should go beyond the limited and general commitments proposed in the WTO Agreement on Electronic Commerce and instead follow the template of the TFA, by being extensive and specific, and any guidelines or recommendations related to data regulations should be available in one place, both online and offline.

To further improve the situation for businesses, commitments could include making public unofficial translations available in several languages, including English (which continues to be the *lingua franca* of the internet) as well as illustrative, easy-to-understand examples of how data regulations should be applied, based on real-world situations. This would be especially beneficial for SMEs that might lack the resources to hire data governance experts.

Another source of inspiration is the system of WTO notifications. There already exists, in theory, a limited notification requirement regarding data regulations in Art. 3 of the WTO General Agreement on Trade in Services (GATS), though compliance is spotty, at best. Interested countries could use Art. 3 of GATS as a basis for developing a more comprehensive notification requirement and system. This would preferably take place within the WTO, and is another topic where commitments in the proposed WTO Agreement on Electronic Commerce are too general and limited.

If it is not possible to move forward within the WTO (due to objections by other member states), a system similar to the WTO notifications could be established under a different international organization, such as the OECD.

The benefits of a well-functioning system for notifications would not only be in increasing transparency around existing and – especially – proposed regulations on cross-border data flows, but also in building trust and understanding of the different regulatory approaches of the participating countries, a key requirement for any future regulatory harmonisation efforts.

90. Transparency is also a central theme of the Data Free Flow with Trust (DFFT) initiative championed by Japan and endorsed by the G7.

91. Annex to the Protocol Amending the Marrakesh Agreement Establishing the World Trade Organization, Agreement on Trade Facilitation, art. 1.

92. See Chapter 4.2.

Useful, realistic and GDPR-compliant?

This recommendation is **useful** for simplifying navigation of the regulatory landscape even though it does not directly reduce fragmentation. It is **realistic**, as transparency measures have been successfully implemented in other areas of trade policy.

It is important to note, however, that transparency obligations can be controversial, as some developing countries argue that they lack the resources to fulfil such obligations. To meet these objections, a mandate to increase transparency could be coupled with our other recommendation on increasing technical assistance and support for capacity building.

Lastly, it is **GDPR compliant**, as it aligns with the EU's commitment to transparency and accessibility regarding the GDPR⁹³.

Information is usually available in all of the official languages of the EU (which serve as the primary or secondary languages of a large part of the global population), and there should be no obstacle to producing further unofficial translations in other languages, nor in stepping up notification efforts.

Figure 10. Trade policy recommendations for moving forward



93. E.g. Your Europe, 'Data protection under GDPR', accessed 10-09-24 and European Data Protection Board, 'EDP website auditing tool', accessed 10-09-24.

6 Concluding remarks

The economic necessity of cross-border personal data flows for businesses is undeniable, as is the wider economic importance of those same data flows for society, and for future economic growth.

Yet, handling cross-border personal data flows is a challenge for businesses of any size, as they must navigate regulations on the international, national and subnational level to know if – and how – personal data may be transferred to other countries. This global patchwork of regulations has been created by policymakers in different jurisdictions seeking to protect important interests in the digital age, such as privacy, security and economic development.

Those same policymakers have introduced quite steep fines for taking a wrong turn. Thus, in navigating the patchwork, many businesses tend to be overly cautious. Companies doing business in the EU must additionally contend with the GDPR – one of the most restrictive data governance frameworks in the world – under which record-breaking fines have been issued for non-compliance.

There is little appetite for challenging restrictions that guarantee privacy rights, or ensure national security, in order to ease the cost of doing business. What we hope to have shown with this study is that there might not be a need to, either. There are pathways forward for policymakers dealing with digital trade – both inside and outside the EU – to mitigate the negative effects of regulations on cross-border data flows, while leaving those same regulations largely untouched, by ensuring any measures to facilitate cross-border data flows conform to criteria such as being compatible with the GDPR.

This study just offers a few recommendations. There may be other options for moving forward, though they would also have to fit the reality of the current trade policy landscape to be useful. This includes both the challenges that businesses face and the constraints that policymakers must abide by, but we hope that others will also will ponder the different options, and publish their views.

Nevertheless, the options for moving forward under our chosen criteria are limited. Strict regulations, most prominent among them the GDPR, leave little room to manoeuvre. To the EU, this remains an acceptable trade-off to safeguard important values such as privacy rights. The adoption of GDPR-like frameworks in other countries shows that other countries share this perspective, while research shows that strict regulations – like the GDPR – limit both economic opportunities and innovation. The fact that the EU is falling behind in the ‘AI race’ highlights this.

There are clearly limits to the *Brussels Effect*. Some countries are already moving forward with different initiatives to reduce regulatory fragmentation and facilitate cross-border data flows (at least among the participating countries). In these countries, views on the balance between the benefits of data flows and the importance of privacy and security differ from the EU, and they are therefore less constrained by regulations on data flows.

As we move into the future, there is a risk that the world could become divided into separate, and largely incompatible, data governance areas. While such developments may make it easier for businesses to transfer data within these areas it will, conversely, make it harder to transfer data *out* of these areas. Also, for each country that aligns and “locks” their regulatory approach with a framework that is incompatible with the GDPR, any way forward that relies on adequacy decisions becomes that much less viable.

Given the tremendous opportunities promised by technology such as AI, we can be sure that many governments across the globe will continue to regulate by focusing on the implementation of these opportunities, regardless of what happens in the EU.

References

Legal

- Annex to the Protocol Amending the Marrakesh Agreement Establishing the World Trade Organization, Agreement on Trade Facilitation.
- Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559.
- Case C-361/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.
- Charter of Fundamental Rights of the European Union (CFR).
- Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.
- (OECD) Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Publications

- Bradford Anu, *The Brussels Effect: How the European Union Rules the World* (2020).
- Casalini Francesca, Gonzáles López Javier and Nemoto Taku (OECD), *Mapping commonalities in regulatory approaches to cross-border data transfers* (2021).
- Chen Chinchih, Benedikt Frey Carl, Presidente Giorgio, *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally* (2022).
- Digital Policy Alert, *Data Governance Regulation in the G20 – A Systematic Comparison of Rules and Their Effect on Digital Fragmentation* (2023).
- Fefer Rachel F. (Congressional Research Service), *Data Flows, Online Privacy and Trade Policy*, R45584, (2020).
- Ferracane Martina Francesca, Hoek Bernard M., Van Der Marel Erik and Santi Filippo, *Digital trade, data protection and EU adequacy decisions* (2023).
- Hamilton Daniel S. and Quinland Joseph P., *the Transatlantic Economy 2021* (2021).
- National Board of Trade, *A Data Flows Test for the Single Market* (2023).
- National Board of Trade, *Advancing the Green and Digital Transition: Possibilities for an expansion of the WTO Information Technology Agreement, ITA3* (2024).
- National Board of Trade, *Innovation, AI, Technical Regulation and Trade* (2023).
- National Board of Trade, *Making Green Trade Happen – Environmental Goods and Indispensable Services* (2014).
- National Board of Trade, *No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods* (2015).
- National Board of Trade, *No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies based in Sweden* (2014).

- National Board of Trade, *The Cyber Effect – the implications of IT security regulation on international trade* (2018).
- National Board of Trade, *The E-Commerce Negotiations in the WTO – understanding non-participation* (2023).
- McGovern Gerry, *World Wide Waste: How digital is killing our planet – And what we can do about it* (2020).
- McKinsey & Company, *Localisation of data privacy regulations creates competitive opportunities* (2022).
- Ministry of Economy, Trade and Industry (Japan), *Interim Report of the Expert Group on Data Free Flow with Trust* (2022).
- Organisation for Economic Co-operation and Development, *Digital Trade Inventory – Rules, Standards and Principles* (2021).
- Suominen Kati, *The CPTPP's Impacts on Digital Trade and the Path Forward* (2021).
- The International Monetary Fund, the OECD, the United Nations, The World Bank and the World Trade Organization, *Digital Trade for Development* (2023).
- UN Trade and Development (UNCTAD), *Digital Economy Report 2021 – Cross-border data flows and development: For whom the data flow* (2021)
- World Economic Forum, *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows* (2020).
- World Economic Forum, *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows* (2023).

Journal articles

- Al Kez Dizar, M. Foley Aoife, Laverty David, Furszyfer Del Rio Dylan, and Sovacool Benjamin, 'Exploring the sustainability challenges facing digitalisation and internet data centers', *Journal of Cleaner Production*, vol. 371 (2022).
- Chander Anupam, 'Is Data Localisation a Solution for Schrems II?', *Journal of International Economic Law* (2020).
- Geradin Damien, Karanikioti Theano, Katsifis Dimitrios, 'GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech', *European Competition Journal*, vol. 17, no 1 (2021).
- Kuner Christopher, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', *German Law Journal*, vol. 18, no 4 (2017).
- Mattoo Aaditya and Meltzer Joshua P, 'International Data Flows and Privacy: The Conflict and Its Resolution', *Journal of International Economic Law*, vol 21, no 4 (2018).

Media articles

- Deutsche Welle, 'Data centers keep energy use steady despite big growth', <https://www.dw.com/en/data-centers-energy-consumption-steady-despite-big-growth-because-of-increasing-efficiency/a-60444548>, accessed 21-04-24.
- New York Times, 'Google Details, and Defends, Its Use of Electricity', <https://www.nytimes.com/2011/09/09/technology/google-details-and-defends-its-use-of-electricity.html>, accessed 21-04-24.
- New York Times, 'How the English Language Conquered the World', <https://www.nytimes.com/2022/01/18/books/review/the-rise-of-english-rosemary-salomone.html>, accessed 21-04-24.
- Scientific American, 'The AI Boom Could Use a Shocking Amount of Electricity', <https://www.scientificamerican.com/article/the-ai-boom-could-use-a-shocking-amount-of-electricity/>, accessed 21-04-24.

Web sources

- Australian Government – Office of the Australian Information Commissioner, ‘*Australian Privacy Principles*’, <https://www.oaic.gov.au/privacy/australian-privacy-principles>, accessed 21-04-24.
- Baker McKenzie, ‘*Global Data Privacy and Cybersecurity Handbook*’, <https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook>, accessed 21-04-24.
- Data Guidance, ‘*China: Unpacking requirements for Critical Information Infrastructure Operators*’, <https://www.dataguidance.com/opinion/china-unpacking-requirements-critical-information>, accessed 21-04-24
- DLA Piper, ‘*Data Protection laws of the world*’, <https://www.dlapiperdataprotection.com/index.html>, accessed 21-04-24.
- EU Commission, ‘*Adequacy decisions*’, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, accessed 10-11-24.
- European Data Protection Board, ‘*EDP website auditing tool*’, https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/edpb-website-auditing-tool_en, accessed 10-09-24.
- EQS Group, ‘*The Biggest GDPR Fines of 2023*’, <https://www.eqs.com/compliance-blog/biggest-gdpr-fines/>, accessed 21-04-24.
- Financial Times, ‘*Companies face high cost to meet new EU data protection rules*’, <https://www.ft.com/content/od47ffe4-ccb6-11e7-b781-794ce08b24dc>, accessed 21-04-24.
- IT Governance, ‘*How Much Does GDPR Compliance Cost in 2020?*’, <https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020>, accessed 21-04-24.
- Infocomm Media Development Authority (Singapore), ‘*About APEC Cross Border Privacy Rules (CBPR)*’, <https://www.imda.gov.sg/how-we-can-help/cross-border-privacy-rules-certification>, accessed 21-04-24.
- Microsoft, ‘*Microsoft’s commitment to GDPR, privacy and putting customers in control of their own data*’, <https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/>, accessed 21-04-24.
- Noyb, ‘*5 Years of the GDPR: National Authorities let down European Legislator*’, <https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator>, accessed 21-04-24.
- Thierer Adam, ‘*Artificial Intelligence Primer: Definitions, Benefits & Policy Challenges*’, <https://medium.com/@AdamThierer/artificial-intelligence-primer-definitions-benefits-policy-challenges-4c20a1fcf465>, accessed 10-11-24.
- Thierer Adam, ‘*GDPR & European Innovation Culture: What the Evidence Shows*’, <https://medium.com/@AdamThierer/gdpr-european-innovation-culture-what-the-economic-evidence-shows-b19d2309de07>, accessed 10-11-24.
- Your Europe, ‘*Data protection under GDPR*’, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm, accessed 10-09-24.

Sammanfattning på svenska

Summary in Swedish

Gränsöverskridande dataflöden är en grundläggande del av den moderna digitala ekonomin och möjliggör tjänster, varor och innovationer inom bland annat e-handel, artificiell intelligens och molnbaserade lösningar.

Större delen av all världens tjänstehandel sker idag digitalt, men dataflöden är även avgörande för den moderna tillverkningsindustrin, där många processer är helt beroende av dataflöden. Detta gäller allt från forskning och utveckling, till att hantera leveranskedjor och tillverkning.

Trots att det handlar om stora ekonomiska värden (år 2025 så uppskattas den digitala ekonomin utgöra en dryg fjärdedel av världens BNP) och grunden för vår framtida ekonomiska tillväxt, så finns det idag betydande hinder för det fria flödet av data mellan länder.

Fragmenterade och svårtolkade regelverk, och skilda tolkningar av dataskyddslagarna som GDPR, har skapat en komplex och oförutsägbar miljö för handel och innovation. Dessa hinder påverkar inte bara handeln negativt utan även de bredare ekonomiska och sociala fördelarna med digitalisering.

I denna utredning analyserar vi dessa hinder och presenterar ett antal handelspolitiska rekommendationer för att förbättra situationen.

Utredningen inleds med en bakgrundsdel där vi undersöker de underliggande problemen kring gränsöverskridande dataflöden, inklusive hur olika nationella regelverk interagerar och skapar hinder för dataflöden. Här analyseras även de ekonomiska effekterna av dessa hinder och deras inverkan på små och stora företag.

Utifrån vår analys presenterar vi några rekommendationer för att minska fragmenteringen och främja effektivare dataflöden:

- **Gemensamma definitioner:** Genom att utveckla gemensamma definitioner för nyckelbegrepp som "personuppgifter" och "adekvat skydds nivå" så kan de juridiska otydligheterna begränsas för företagen, och de gemensamma definitionerna kan även bidra till att bygga förtroende mellan handelspartner.
- **Fler (och snabbare) adekvansbeslut:** Genom åtgärder som ökar transparensen och uppmuntrar EU-kommissionen att inleda fler adekvansundersökningar så kan antalet länder som erkänns som adekvata av EU växa, vilket i sin tur leder till ett större område där data kan flöda både fritt och integritetssäkert.
- **Tekniskt stöd till utvecklingsländer:** Genom kapacitetsutvecklingsprojekt så kan utvecklingsländer få stöd att utveckla och anpassa sina dataskyddsramverk till globala standarder (som GDPR), vilket skulle innebära att fler aktörer kan delta i den digitala ekonomin.
- **Ett "dataflödestest":** Onödiga handelshinder kan förebyggas genom ett test som hjälper beslutsfattare i EU att väga för- och nackdelar med nya regler på det digitala området. Dataflödestestet kan även fungera som en modell för andra regioner.
- **Transparens och tillgänglighet:** WTO:s system med notifieringar och transparens kan användas som en inspirationskälla för åtgärder som gör regler kring dataflöden mer tillgängliga för företagen, och lättare att förstå. Sådana åtgärder skulle vara särskilt värdefulla för små och medelstora företag genom att minska kostnader och förenkla efterlevnad.

I utredningen betonar vi att dessa rekommendationer inte syftar till att lösa alla problem kring gränsöverskridande dataflöden, men de erbjuder praktiska och genomförbara steg för att minska hinder och fragmentering, som dessutom inte bör hamna i konflikt med GDPR och EU:s regler kring skyddet av den personliga integriteten.

Våra rekommendationer är av särskild relevans för beslutsfattare i EU, men de föreslagna åtgärderna har också globala implikationer. Genom att stärka samarbetet mellan olika datajurisdiktioner och intressenter, inklusive nationella myndigheter, internationella organisationer och näringslivet, går det att skapa regelverk som bättre tar tillvara på de stora ekonomiska och sociala fördelarna med digitaliseringen. I utredningen betonar vi också vikten av att inkludera utvecklingsländer i denna process för att säkerställa en mer jämlik global digital ekonomi.

The National Board of Trade Sweden is the government agency for international trade, the EU internal market and trade policy. Our mission is to facilitate free and open trade with transparent rules as well as free movement in the EU internal market.

Our goal is a well-functioning internal market, an external EU trade policy based on free trade and an open and strong multilateral trading system.

We provide the Swedish Government with analyses, reports and policy recommendations. We also participate in international meetings and negotiations.

The National Board of Trade, via SOLVIT, helps businesses and citizens encountering obstacles to free movement. We also host several networks with business organisations and authorities which aim to facilitate trade.

As an expert agency in trade policy issues, we also provide assistance to developing countries through trade-related development cooperation. One example is Open Trade Gate Sweden, a one-stop information centre assisting exporters from developing countries in their trade with Sweden and the EU.

Our analyses and reports aim to increase the knowledge on the importance of trade for the international economy and for global sustainable development. Publications issued by the National Board of Trade only reflect the views of the Board.

The National Board of Trade Sweden, February 2025. ISBN: 978-91-89742-53-6

