



Department for
Science, Innovation
& Technology

TOWARDS A SUSTAINABLE, MULTILATERAL, AND UNIVERSAL SOLUTION FOR INTERNATIONAL DATA TRANSFERS

A report by the UK Government's
International Data Transfer Expert Council

November 2023

CONTENTS

	PAGE
1. MINISTERIAL FOREWORD	1
2. THE UK GOVERNMENT'S INTERNATIONAL DATA TRANSFERS EXPERT COUNCIL	2
3. EXECUTIVE SUMMARY AND RECOMMENDATIONS	3
4. INTRODUCTION	10
5. THE VALUE AND IMPORTANCE OF INTERNATIONAL DATA TRANSFERS – EVIDENCE AND CASE STUDIES	2
6. TRUSTED GOVERNMENT ACCESS TO DATA	9
7. UK GOVERNMENT TACTICS AND STRATEGY FOR ACHIEVING ITS GOALS	16
8. MULTILATERAL SOLUTIONS FOR SUSTAINABLE AND SCALABLE INTERNATIONAL DATA TRANSFERS	24
9. EXPERT COUNCIL BIOGRAPHIES	33



Ministerial foreword

In our globally connected world, data access and data use are foundational to economic growth, scientific research, innovation and driving the productivity of businesses. Indeed, in 2021, the UK data economy was estimated to represent 6.5% of GDP, and at least 85% of UK service exports worldwide were data-enabled. Data access is also critical to developing and using increasingly commonplace digital technologies such as AI, and more frontier technologies such as quantum tech and supercomputers.

The pace of technological development and innovation is accelerating and offers the potential to bring huge new opportunities across government, business, and public sectors. However, the transfer and security of data is not keeping pace and is in fact increasingly subject to differing legal and regulatory requirements, reducing the societal and economic benefits of data and digital technologies.

In this context, the current fragmented approach to the global data flows system is unsustainable. Legal uncertainty and burdensome compliance have become core features of the international data driven economy - stifling research, innovation, trade, and growth. I often hear from organisations that face too many challenges and barriers to seamless cross-border data flows, sharply reducing their capacity to trade, lowering their productivity, and raising prices for downstream industries that increasingly rely on data.

These challenges cannot be resolved by countries working alone. As we have set out in the UK's National Data Strategy, we are committed to championing international flows of data working with our international partners. This includes working to promote interoperability between different data protection regimes.

This ambition underpins the UK's Data Protection and Digital Information Bill (No.2), seizing on our opportunity to access billions of pounds in the booming global data driven trade, including by clarifying our international transfers regime for building data bridges to secure the close, free and safe exchange of data with other trusted allies.

We were delighted to announce a UK data bridge with the Republic of Korea last November. Maintaining this momentum, on 12 October 2023, the UK-US data bridge came into force, allowing certified organisations to easily transfer personal data from the UK to the US.

Beyond updating our regulatory framework, we are championing initiatives in multilateral fora for more global scalable and multilateral solutions. We helped negotiate the OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities, and used our G7 Presidency to set out a Roadmap for Cooperation on Data Free Flow with Trust and collaborated with the ICO on the development and implementation of the International Data Transfer Agreement (the first updated transfer tool since EU Exit). Our recent accession to associate status in the Global Cross Border Privacy Rules (CBPR) Forum also presents the UK with an opportunity to help drive cooperation with member nations on international data flows, while maintaining high data protection standards.

As we continue to develop ambitious policy, the government should learn from experts and stakeholders to develop solutions to the global challenges we all face regarding international data flows. It is inherent upon us to seek and understand the diversity of views amongst those who feel the impacts of our policy and action on the ground, to shape and inform our thinking.

This is why, in January 2022, the UK government launched the International Data Transfers Expert Council, bringing together 20 world-leading data experts from across academia and industry representative bodies. We gratefully received this independent and honest advice on international data transfer issues, and I would like to offer my sincere thanks to the members of the Expert Council for their valuable insight and expertise which underpins this report.

We look forward to considering this report and continuing to work with the Expert Council going forward to deliver our shared ambition to build a more fit for purpose global data flows system.

THE UK GOVERNMENT'S INTERNATIONAL DATA TRANSFERS EXPERT COUNCIL



The UK Government established the International Data Transfers Expert Council (the Council) in January 2022, coordinated by the Department for Science, Innovation and Technology (previously by the Department for Culture, Media and Sport at the time of the Council's inception).



The purpose of the Council is to provide independent advice to the UK Government in its mission to unlock the benefits of free, responsible, and trusted international personal data transfers, while at the same time maintaining high standards of data protection and regulatory/government cooperation for cross-border protection of citizens' rights.



Experts on the Council were selected from among leading data and privacy practitioners, not-for-profits, academia, law and industry, both from the UK and elsewhere around the world. All work at the forefront of this rapidly moving area of law and policy. In addition to expertise in data protection and data flows, their experiences cover a range of areas including patient healthcare, scientific research, finance, and technology such as cloud computing, cybersecurity, and artificial intelligence.



This Report, including its findings and recommendations, are based on the Council's work, research, and meetings since its inception. The Council members were split into four subgroups, each of which considered a specific set of questions. The Report is therefore not intended to be a comprehensive review of the current landscape in international data transfers and existing international fora in this field, but rather captures the discussions between Council members focused on their own areas of expertise. The Council hopes this Report will be a springboard for further discussion.



The Report contains the Council's independent recommendations to the UK Government and the international community and encourages a call to action globally: to start a constructive conversation and lay foundations for a future framework for trusted and responsible flows of personal data that benefits everyone.

EXECUTIVE SUMMARY AND RECOMMENDATIONS

Characteristics of a sustainable solution for international transfers of personal data

There is currently no central governance body that provides a forum for governments and organisations to come together and agree on a practical framework in the field of international data transfers, so there is an urgent need for leadership and collaboration in this space. This stands in contrast to other areas, such as financial services, trade, or intellectual property, where global centralised bodies exist, namely the Financial Stability Board, the World Trade Organisation and World Intellectual Property Organisation.

None of the existing multilateral fora engaged in the field of personal data is currently globally empowered and positioned to put in place universally acceptable multilateral solutions for international data transfers. The Council of Europe, the Organisation for Economic Cooperation and Development (OECD), the Global Cross-Border Privacy Rules Forum (Global CBPR Forum), and the G7 all offer possibilities in this regard. However, these existing multilateral fora are not inclusive enough, and do not go far enough, to address the wider fragmentation in the existing governance landscape for personal data. They do not deal with the barriers to international data transfers as effectively as possible, nor build new solutions and frameworks to address the issue. There is a danger that the world is headed towards a “data blocs” scenario, with declining multilateralism and increasingly diverging standards. This would result in further reductions in trust and restrictions to data flows, thus impeding economic and societal progress for all.

In order to unlock the benefits of international data transfers while maintaining high standards of data protection, the Council believes that it is necessary to identify and define the characteristics of the most appropriate solution to deliver this aim. This solution should be viable in the short term, sustainable in the long term, and as universally acceptable as possible.

In its discussions to develop the recommendations in this Report, the Council agreed that a sustainable solution for international data transfers should:

- **Have strong political endorsement** – including being underpinned by clear political commitment and binding agreements.
- **Be risk-based** – accepting that absolute equivalence of laws is unfeasible and looking at both the laws and practices of a country in determining whether their protections for personal data are robust. It should assess the likelihood and severity of risks and harms to individuals, as well as technical protections that can be implemented to mitigate the risks, such as encryption, confidential computing, or other privacy-enhancing technologies. The focus should be on addressing reasonably foreseeable risk of harm rather than eliminating all theoretical risk.
- **Be accountability-based** – recognising that organisations transferring personal data remain responsible for implementing proportionate, risk-based, and effective safeguards so there is reasonable protection for personal data wherever it travels. There should be effective oversight to ensure this accountability.
- **Be interoperable and outcomes-focused** – rather than focusing on the terminology or prescriptive rules and regulations, the solution should be based on common agreement of desirable outcomes. This would mean not insisting upon identical rules and requirements and, according to different contexts and specificities, allowing countries to determine different ways to provide equivalent outcomes of effective protection for personal data and rights of individuals, whilst realising the benefits from use of personal data.

- **Consist of multiple mechanisms** – noting that no single tool or mechanism can provide the panacea for international data transfers. Instead, while working on a longer-term, sustainable multilateral solution, the focus should be on the expansion, and mutual recognition of suitable transfer tools (legal, organisational and/or technical) and regulatory/governmental cooperation on cross-border enforcement. This would provide a more uniform and balanced global system, suitable for organisations of all sizes and sectors.
- **Follow incentive-based enforcement** – allowing demonstrated compliance to be taken into account in enforcement decisions.
- **Be scalable** – encouraging participation from nations and organisations of all sizes with an approach that is not unduly burdensome for smaller nations and small to medium size organisations.

Recommendations

The Council offers the following recommendations, supporting short-, medium-, and long-term action, to promote and facilitate the development of a global solution on international data transfers with the characteristics outlined above. These recommendations represent options for routes the UK Government could seek to pursue and lead on internationally and are not necessarily all to be advanced simultaneously.

RECOMMENDATION #1:

The UK should further advance its unique position and provide global leadership to resolve global challenges related to international data transfers, driving stability to enable the benefits of international data transfers while emphasising strong, outcome-oriented protections.

Advance an even bolder public narrative, both domestically and internationally; promoting the characteristics of a sustainable solution outlined above and emphasising the wider benefits of international data transfers to the economy, society, and individuals' lives. Examples of key areas of such benefits are (1) online safety of children, (2) cybersecurity, and (3) algorithmic development in artificial intelligence. **[Short-term]**

Actively encourage regulators, policymakers, and lawmakers to incentivise, promote, and motivate organisations to implement and demonstrate accountability that enables responsible and trusted international data transfers. This will serve as an impetus for organisations to compete in a race to the top, that would improve overall market behaviours over time. **[Short-term]**

Facilitate international engagement on international data transfers, serving as a convener of collaborating stakeholders and bridging gaps between different models/perspectives, including seeking to foster international regulatory/governmental cooperation on the cross-border enforcement of privacy/data protection infringements. **[Medium-term]**

Champion a truly inclusive approach to the conversation on international data transfers, increasing engagement with high-growth countries, smaller to medium-sized businesses, civil society groups, standards bodies, and non-governmental organisations (NGOs) in the design and delivery of policies and laws/regulations on international data transfers. **[Medium-term]**

RECOMMENDATION #2:

Build upon current momentum around trusted government access to personal data held by the private sector.

Continue to engage via the OECD on the issue of trusted government access to personal data held by private sector entities, and on the expansion of the adoption of the OECD's Trusted Government Access Principles (TGA Principles) among non-OECD countries that are capable of meeting the principles. **[Short-term]**

Lead by example by publishing – in plain and accessible terms – how the UK meets the TGA Principles, encouraging other countries to do similar. Explore how the UK, either working alone, with other countries, and/or with multilateral fora like the OECD or the G7, could maintain a 'library' of such disclosures, which would promote transparency and trust. **[Short-term]**

Work to foster a more consistent global dialogue about where surveillance and government access could pose a risk of harm, taking into account authoritarian practices, government secrecy, and poorly constrained government access to personal data. **[Short-term]**

Explore how the impact of the TGA Principles can be strengthened by more and more countries choosing to follow and implement the TGA Principles in their own governmental surveillance practices. Consider how TGA Principles could be paired with, referenced or leveraged by global data flows systems, like the CBPR. **[Medium-term]**

Encourage connectivity, engagement, and sharing of experiences between international personal data protection/privacy regulators and the broader law enforcement and intelligence community in order to grow mutual understanding and embed privacy considerations more integrally into the broader system of government access requests. **[Medium-term]**

Socialise the TGA Principles and the importance of trusted government access to data with civil society and businesses. **[Medium-term]**

Promote the accountability of organisations and governments for implementing the TGA Principles. **[Medium-term]**

RECOMMENDATION #3:

Champion the growth and expansion of organisational accountability as a basis for trustworthy international data transfers.

Noting that many data protection authorities are independent of governments in their jurisdictions (with the Information Commissioner's Office in the UK being no exception), encourage data protection authorities to incentivise good organisational practices and accountability in international data transfers. This could be achieved by, for example, including measures such as certifications and trustmarks as factors when considering enforcement, engaging with regulators to adopt certification mechanisms in respect of international data transfers. The aim of policy makers and regulators should be to deliver long term positive changes in behaviours, contribute to legal certainty and promote global adoption of best practice. **[Short-term]**

Build on the lessons of twenty years of Binding Corporate Rules (BCRs) in Europe to urge the Information Commissioner's Office to take the lead in the advancement of a streamlined approval and adoption process for BCRs, which facilitates regulatory approvals and encourages organisations of all sizes to adopt this model. **[Short-term]**

Seek to "multilateralise" transfer mechanisms by reimagining and evolving BCRs and Standard Contractual Clauses (SCCs),¹ as tools to be negotiated and recognised at the international level rather than established by and recognised within a particular region or a country. In particular, this may include working with international partners to promote mutual recognition of SCCs and BCRs and considering how BCRs may evolve as a transfer mechanism between BCR-approved companies and be certifiable by a third party on a global scale. **[Medium-term]**

Explore soft and hard regulatory incentives for reliance on recognised international data transfer mechanisms (especially those that are accompanied by more robust ex ante scrutiny, such as BCRs). **[Medium-term]**

Where multilateral transfer mechanisms already exist, dedicate resources to ensuring effective secretariat funding and control over programme requirements and recognition of certification under those mechanisms, to maintain an updated system which can be scaled for countries of differing capacities around the world and will enable uptake of high-level, global privacy protections among smaller to medium-sized enterprises. **[Medium-term]**

Help and support countries with nascent data protection regimes, especially in high-growth countries, to grow the foundations for trusted transfers of personal data by conducting capacity building for privacy regulation formulation, implementation and enforcement, outreach to local business communities on privacy compliance needs and local individuals on privacy concerns, and support for accession to multilateral organisations or agreements such as the Global CBPR Forum or TGA Principles. **[Medium-term]**

With due regard for their independence, encourage cooperation between national data protection regulators to enforce data protection decisions cross-border. Focus efforts on setting up better mechanisms for cooperation between regulatory authorities to ensure there is adequate protection of data wherever it travels. **[Medium term]**

¹ BCR are data protection policies to which companies within the same corporate group adhere, whereby they commit to providing adequate safeguards for making international data transfers. SCCs are contractual clauses which likewise ensure

that adequate data protection safeguards are in place to allow transfers overseas.

RECOMMENDATION #4:

Engage in standards work to operationalise international data transfer protections clearly.

Explore certification to international technical standards such as ISO, ETSI or other recognised industry standards with appropriate scope being approved as certification mechanisms to enable transfers from the UK. Similarly, seek the development of codes of conduct (such as in cloud computing) to enable transfers from the UK, with a view to then engaging with other personal data protection policymakers and regulators to encourage their recognition of such certifications and/or codes and incentivising adherence to them. **[Short-term]**

Supporting the British Standards Institute (or other standard bodies) in evolving technology-neutral and internationally accessible mapping, modelling and methodologies to better enable organisations and governments to understand their accountable practices for international data transfers. **[Medium-term]**

RECOMMENDATION #5:

Pursue an active multifaceted international strategy to encourage discussion of the topic in relevant multilateral fora.

Continue to invest and dedicate attention to work advancing responsible international data transfers in multiple multilateral fora -- especially the G7 and OECD -- by actively supporting the adoption and operationalising of "data free flow with trust" and promoting scalability of mechanisms like the TGA Principles to non-signatory countries. The approach should be tailored to the opportunities and challenges of each forum and should encourage targeted and meaningful cooperation between different international fora according to their specialism. **[Short-term]**

The UK Government may be able to build on the current momentum to build an international approach to artificial intelligence (AI) governance at the UK hosted AI governance summit this autumn, as AI is closely linked to global data flows and depends upon access, use and sharing of data across borders. **[Short-term]**

Work through multilateral fora like the World Bank, the Inter-American Development Bank, the Commonwealth, the Council of Europe, and the UN, to promote the development of personal data protection regimes across the globe and widen participation in multilateral conversations about international data transfers. **[Medium-term]**

Establish a binding treaty between countries that guarantees appropriate protections for personal data and secures international consensus, which would provide true stability for trusted and responsible international data transfers. Such an outcome is not realistic in the foreseeable future, but the UK should consider its own vision for such a treaty. **[Long-term]**

RECOMMENDATION #6:

Complement multilateral work with focused bilateral engagement on transfers of personal data transfers internationally.

Resource and scale efforts to establish data bridge agreements, setting an ambitious, but realistic, target list of priority countries.

[Short-term]

Maintain strong communication and collaboration with the European Union on personal data protection and transfers; approaching the common challenges in a spirit of cooperation, transparency, and trusted partnership. **[Short-term]**

Establish a data bridge with the United States, building on the June 2023 announcement of an agreement in principle contained in the Atlantic Declaration and the EU-US Data Privacy Framework adopted by the EU in July 2023, maintaining a strong partnership and collaboration to promote and operationalise free flows of personal data with trust. **[Short-term]**

Engage with counterparts internationally who are developing and updating data protection regimes, including sharing the UK's experience in weighing law enforcement, national security, economic, and privacy considerations in the development of a regime for free-flows of personal data. **[Short-term]**

Engage with, and learn from, countries that considered, but then shifted away from, strict data localisation requirements (Indonesia, Brazil, Kenya). These conversations will offer insight on how to advance most effectively the goal of "data free flow with trust", including by understanding the pitfalls of localisation. **[Medium-term]**

RECOMMENDATION #7:

Contribute to shaping the evolving approach and design of the governance of the Global CBPR system, with a view to making it a more meaningful and widely accepted basis of a true multilateral solution.

Use the UK's Associate status in the CBPR Global Forum to work with Global Forum Members to shape governance and design of the Global CBPR and Global Privacy Recognition for Processors (PRP) Systems and be open to considering full membership of the Global CBPR Forum if sufficient progress to enhance CBPR standards is achieved and industry uptake is increased. **[Short-term]**

Promote and contribute to developing the potential of the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Enforcement Arrangement. **[Short-term]**

Work with Global CBPR Forum members to understand past barriers to countries and companies joining the Global CBPR system, and work with stakeholders to creatively address those barriers in the Global CBPR system. **[Short-term]**

Further use the UK's industry and global relationships to build broader awareness and

momentum for the Global CBPR system, including in countries in Latin America, Asia and the Pacific, the Middle East, and Africa. **[Short-term]**

Work with international partners to develop tools for organisations who follow GDPR-style domestic regimes to facilitate international transfers to CBPR and PRP certified organisations. **[Medium-term]**

Work with Global CBPR Forum members to enhance the requirements of the Global CBPR system beyond the APEC requirements, in line with international norms around privacy expectations and compliance requirements. **[Medium-term]**

Work to bridge the Global CBPR system with the GDPR, including through engagement with the European Commission and Council of Europe to promote interoperable cross-recognition of the Global CBPR and any possible transfer certification tied to Convention 108+ once the treaty is in force. **[Medium-term]**

RECOMMENDATION #8:

Continue to dedicate resources to solving challenges in international data transfers.

Continue to engage with stakeholders to gather and publicise best practice and seek new and innovative perspectives on approaches that the UK Government could take. **[Short-term]**

Make available relevant data and modelling tools to support empirical research on the social and economic impacts of data protection, digital trade, and the value of international data transfers to inform public policy and facilitate international discussion. **[Short-term]**

Use the UK Business Data Survey (UKBDS) to gather further case studies and improve the evidence base on international data transfers to and from the UK. **[Short-term]**

Continue the ongoing work of the Council, with a rotating group of experts that reflects broad geographical and societal interests, to act as a resource for the UK Government and ensure the UK's work in this space remains informed by multi-stakeholder input. Empower the Council to provide advice, support, and act as a centre of excellence in respect of international data transfers policy, law, and implementation. The Council should have the ability to provide further recommendations, reports, and reviews, with DSIT continuing to facilitate the meetings of the Council. **[Medium-term]**

Conclusion

The Council looks forward to the UK Government's response to these recommendations, and to continuing its close work with the UK Government in the coming months to take forward the actions and recommendations in this Report.

The next iteration of the Council should focus on generating ideas and proposals for the implementation plan that will take forward the recommendations in this Report.

INTRODUCTION

Data are essential to all businesses in the United Kingdom.² In 2022, 85% of UK businesses, large and small, stated that they rely on digital data,³ which inevitably means they depend on the movement of data. This is a global trend. Multiple McKinsey Global Institute studies detail the digitalisation of the global economy and that, while global goods trade is flattening and value chains are becoming more regional, data flows and services are rapidly growing as they reshape global trade and economic integration.⁴ DSIT estimates that the value of UK data-enabled trade in 2021 was £387bn, of which £259bn was exports and £128bn was imports.⁵ The UK's future economic prosperity depends in no small part on its strategy for transfers of data, including personal data, given the role of those transfers in the functioning and expansion of the digital economy.

International flows of and access to personal data are also the foundation of societal and human progress. They enable cooperation and communication, fuel cutting edge medical and scientific research, drive the exchange of ideas, and shape common values. Flows of personal data support digital inclusion, by allowing all people and nations an equitable, easy, and low-or-no cost way to access information, knowledge, education, health, government, and other services critical to democratic countries such as voter registration and even voting.

As important as the data flows themselves is building and maintaining trust in those data flows. Trusted data flows depend upon organisations being held accountable for data use and sharing, complying with the law, and adopting responsible practices when transferring data within and outside national borders. Trust also means having legal certainty and appropriate regimes, rules, and protections for data as it flows across national borders including effective enforcement and protection of individual rights.⁶ Legal protections and accountability must flow with the data. This is increasingly referred to as “data free flow with trust”, a concept introduced during the World Economic Forum Annual Meeting 2019 in Davos-Klosters by the late Prime Minister Shinzo Abe,⁷ which applies to all data types and is not limited to personal data. Since Prime Minister Abe's first use of the term “data free flow with trust”, the G7 have adopted this terminology, and it is frequently used to describe an ideal outcome for international data transfers.

Each nation has different data protection rules, shaped by its own culture and values, but frequently sharing common characteristics. This leads to multiple (and sometimes conflicting) rules on transferring personal data internationally. This legal fragmentation potentially undermines global data transfers and the broader digital economy.

Global data flows can be undermined by measures put in place by governments requiring

² The focus of this Report is on international transfers of personal data (referred throughout as international data transfers) given the importance of personal data to the economy and the growing restrictions on its use, sharing, and transfers across borders. However, it is recognised that global flows of non-personal data are also critical for economic and societal growth, and they are also sometimes subject to similar restrictions that impact transfers of personal data. Consequently, within this Report some recommendations will be specific to international transfers of personal data, and some may be applied to data more broadly.

³ “UK Business Data Survey 2022” [GOV.UK](https://www.gov.uk/government/statistics/uk-business-data-survey-2022/uk-business-data-survey-2022--2), June 9, 2022. <https://www.gov.uk/government/statistics/uk-business-data-survey-2022/uk-business-data-survey-2022--2>

⁴ See, for example, “Digital Globalization: The New Era of Global Flows”, McKinsey Global Institute, 2016 <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20Globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.pdf>. “Globalisation in Transition: the Future of Trade and Value Chains”, McKinsey Global Institute, 2019 <https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains> and “Global Flows: the Ties

That Bind in an Interconnected World”, McKinsey Global Institute, 2022

<https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world>

⁵ DSIT internal analysis on the world total of UK services exports, based on 2021 ONS published statistics, in sectors defined as data-enabled by UNCTAD (United Nations Conference on Trade and Development). Data-enabled services are those principally or largely enabled by information and communication technologies (ICT) such as finance and telecommunications.

⁶ “Recommendation of the Council on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy” 2007, Organisation for Economic Cooperation and Development <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352>

⁷

https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data_Flows_2020.pdf

organisations to store data within a country's borders. This is known as “data localisation”. While there is no universally accepted recognised definition of data localisation, a recent one set out in a 2022 OECD⁸ report is a good rule of thumb - “data localisation’ refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction”. The number of data localisation measures in force around the world has more than doubled in four years. In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions and dozens more are under consideration.⁹

Data localisation laws/measures come in many forms and are imposed for a range of motivations. Some data localisation requirements are cross-sectoral, while others only apply to specific types of data. Some allow international data transfers but require organisations to store a copy of the data locally. Many data restrictions are a result of growing concerns from some governments, or their citizens and residents, about other governments’ excessive access to personal data for national security and intelligence or law enforcement purposes. However, it is often an oversimplification to assume that imposing data localisation requirements will address concerns over government access to data.

Organisations increasingly find themselves caught in the middle of the significant challenge of managing multiple, often conflicting, legal requirements that impact effective and trusted international data transfers. Issues include:

- fragmented national legal requirements;
- organisations being expected yet unable (given a lack of transparency) to assess the risk of government access to data and the data recipient countries’ laws/practices in that regard;
- increasing costs vis-a-vis the resources required to understand and comply with international data transfer restrictions or data localisation requirements¹⁰;
- some regulators’ zero-risk approaches to international data transfers (i.e., giving little to no consideration of likelihood or severity of harm, instead considering transfers to be unlawful even if the risk is theoretical, not probable or realistic) due to a lack of trust in other countries’ data protection and government access regimes; and
- unjustified or unrealistic data localisation rules.

All of these issues hinder efforts to create global interoperability between, and mutual recognition of, different international data transfer mechanisms, such as the Global Cross-Border Privacy Rules (CBPR). Furthermore, organisations find themselves in the untenable position of being held responsible for concerns that are not about their own practices, but rather the geopolitics of trust between nations and/or their regulators. Data localisation requirements are difficult, if not impossible, for organisations in the private sector participating in international data transfers to resolve on their own.

⁸ Svantesson, D. (2020-12-22), “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, OECD Digital Economy Papers, No. 301, OECD Publishing, Paris. <http://dx.doi.org/10.1787/7fbaed62-en>

⁹ Cory, Nigel, and Luke Dascoli. “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them.” Information Technology and

Innovation Foundation (ITIF), July 19, 2021.

<https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

¹⁰ The 2021 IAPP-EY Privacy Governance Survey found complying with cross-border data transfer laws to be privacy professionals’ most difficult task, see https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

The 2023 OECD report on opportunities and obstacles to “data free flow with trust” provides evidence on businesses’ and legal practitioners’ overall negative perception of the state of regulation of international data transfers (personal and non-personal), as well as the report assessing the growth of legal fragmentation, barriers to “data free flow with trust”, varying and often inconsistent data transfer mechanisms, and legal uncertainty around data flows. The OECD report also highlights the importance of legal and regulatory frameworks remaining attuned to recent or developing technologies and how these technologies, such as artificial intelligence, blockchain and cloud computing, will impact data flows and international data transfers.¹¹

Since the free flow of data with trust is the bedrock of the global digital economy,¹² barriers to this are economically damaging.¹³

Organisations of all sizes and from all sectors report the growing risk and impact that legal/regulatory restrictions have on their ability to share and transfer personal data across borders, in particular for everyday real use cases that by default depend on international data transfers. Restricting “data free flow with trust” has a significant impact on a nation’s economy – sharply reducing its total volume of trade, lowering its productivity, and increasing prices for downstream industries that increasingly rely on data.¹⁴ For instance, the Information and Technology Innovation Foundation (ITIF) has found that a 1-point increase in a nation’s data restrictiveness results in a 7 percent decrease in

its gross trade output, a 2 percent decrease in its economy-wide productivity, and a 1.5 percent increase in its prices of goods and services among downstream industries.¹⁵

Finally, and importantly, the existence of barriers to data flows can also have negative implications for countries’ cooperation on public policy, science and medical research, and their ability to respond to upcoming threats such as climate change and future pandemics.¹⁶ The Centre for Information Policy Leadership recently published a paper outlining the real-life harms that would result for organisations, people, and society if international data transfers are halted, providing examples (such as online education services, fraud prevention and cyber security) where data must flow by default.¹⁷

The global nature of the internet and data flows means that data-related legal fragmentation and conflict cannot be resolved through domestic law reforms, or through bilateral initiatives between countries, alone. The international community is at a critical point where it should encourage global commitments to “data free flow with trust”. These commitments should be implemented with practical, sustainable, and multilateral solutions for international data transfers, with agreed and recognised standards to achieve the requisite trust for data to flow freely and responsibly. The Council believes that this is a pivotal moment for the UK, and its international partners, to work together to set shared goals and a plan to build a sustainable framework for trusted international data transfers that benefits all nations and their peoples.

¹¹ “Moving Forward on Data Free Flow with Trust”, OECD Digital Economy Papers, April 2023. <https://www.oecd-ilibrary.org/docserver/1afab147-en.pdf?expires=1685630540&id=id&accname=guest&checksum=1BD51A72A919F578C2E18D6D143655EF>

¹² Department for International Trade. “G7 Trade Ministers’ Digital Trade Principles.” GOV.UK. GOV.UK, October 22, 2021. <https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles>.

¹³ See footnote 9 above and McKinsey Global Institute, “Global Flows: The Ties That Bind in an Interconnected World,” McKinsey & Company, November 15, 2022, <https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world>.

¹⁴ See footnote 9 above.




¹⁵ *ibid.*

¹⁶ For examples of these real-life use cases, see “The Real Life Harms of Data Localisation Policies”, The Centre for Information Policy Leadership, April 2023 accessible at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf and Nigel Cory, “Viruses Cross Borders. To Fight Them, Countries Must Let Medical Data Flow, Too”, ITIF, May 7, 2020.

<https://itif.org/publications/2020/05/07/viruses-cross-borders-fight-them-countries-must-let-medical-data-flow-too>

¹⁷ “The Real Life Harms of Data Localisation Policies”, The Centre for Information Policy Leadership, April 2023 accessible at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf

THE VALUE AND IMPORTANCE OF INTERNATIONAL DATA TRANSFERS – EVIDENCE AND CASE STUDIES

-  The need for evidence
-  Evidence and case studies on data flows
-  Key findings

The need for evidence

For the UK to continue to develop and expand its capability and keep pace with an ever-evolving global environment, it needs access to the widest range of evidence possible to support DSIT’s work on UK data bridges¹⁸, alternative transfer mechanisms, and how it can best identify future jurisdictions as priority international data transfer partners.

There is limited research on the exact value of international data transfers, though what is available demonstrates its importance. Evidence from 2022 indicates that 13% of all UK businesses send or receive data internationally (equivalent to over 700,000 businesses), rising to 41% of large businesses. These businesses disproportionately represent an estimated 28% of all UK business turnover and 25% of workforce employment.¹⁹ DSIT research estimates the value of UK data transfers with the EU at £2 billion over 10 years.²⁰ Naturally, these economic benefits have significant corresponding social benefits for individual citizens throughout the UK.²¹

While OECD research from 2020²² has shown that the volume of transferred data is not necessarily a useful indicator when trying to establish the value of cross-border data flows, the point remains that even statistics on the volume of data transferred are not easily available. As a result, research on the question of value has suffered.



“To develop and expand the UK’s capability and keep pace with an ever-evolving global environment, the UK needs access to the widest range of evidence possible”

¹⁸ This concept is more commonly known in EU parlance as an adequacy decision.
¹⁹ <https://www.gov.uk/government/statistics/uk-business-data-survey-2022/uk-business-data-survey-2022--2#summary>
²⁰ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1151358/data_protection_and_digital_information_bill_impact_assessment_march_2023.pdf
²¹ New Economics Foundation; UCL European Institute ‘The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to secure an EU Data Adequacy Decision’, 2020, https://neweconomics.org/uploads/files/NEF_DATA-INADEQUACY.pdf
²² Nguyen, D. & Paczos, M. (2020). Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective. OECD Digital Economy Paper No. 297. https://www.ospi.es/export/sites/ospi/documents/documentos/Measuring_the_Economic_Value_of_Data.pdf

To support Mission 5 of the National Data Strategy - Championing International Data Flows²³ - DSIT uses a range of existing evidence, sourced both internally through initiatives such as the UK Business Data Survey (UKBDS), as well as utilising externally available evidence. The findings of business interviews as part of the UKBDS show a lack of understanding among businesses of what an international data transfer is and what tools exist to make them. Similarly, the quantitative survey part of the UKBDS found that only 9% of businesses that handle personal data and transfer data overseas said they knew a great deal.²⁴ In a world that is becoming ever more reliant on data, and as the digital economy continues to grow, the Council is conscious that the evidence base for data flows needs to be widened and thinking on evidence and analysis of data transfers needs to be driven forward at pace.



“The findings of business interviews as part of the UKBDS show a lack of understanding among businesses of what an international data transfer is and what tools exist to make them”

Evidence and case studies on data flows

The Council considered a variety of case studies that illustrate the benefits and challenges in establishing secure and trusted international data transfer mechanisms.

The UK response to the Covid-19 pandemic

From 2020-2022, the UK required relevant organisations to disseminate health data to support the UK’s response to the Covid-19 pandemic.²⁵ There was strong community support for the use of data sharing for public health purposes, provided the data remained appropriately secure. Data was shared with different stakeholders and services that relied upon globally distributed systems or, for example, national medical regulatory bodies or the World Health Organisation. The accelerated data flows produced numerous benefits, such as tracking the spread of the virus, managing resources, delivery of healthcare to individuals, and medical research. The accelerated sharing was limited to a fixed period, records were required to be maintained, there was effective messaging to ensure the public was aware of the nature and extent of data sharing, and the UK Government assisted organisations by providing template privacy notices. However, more could have been done. A recent report by the Institute for Government found that, “data sharing successes during the pandemic proved that there was an unusually urgent need to build new services quickly. This would have been easier had more organisations been prepared to share data, either through established data sharing frameworks or through building relationships and trust in mutual data practice.”²⁶ International data exchange is especially important in the field of health research, even outside of exceptional cases such as the Covid-19 pandemic.²⁷

²³ National Data Strategy - GOV.UK <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#missions>

²⁴ "International transfers of personal data for health research following Schrems II: a problem in need of a solution" <https://www.nature.com/articles/s41431-021-00893-y>

²⁵ See <https://www.england.nhs.uk/wp-content/uploads/2022/07/COPI-notice-to-nhs-england-improvement-covid-19.pdf>

²⁶ https://www.instituteforgovernment.org.uk/sites/default/files/2023-02/Data%20sharing%20during%20coronavirus%20lessons%20for%20government_2.pdf

²⁷ "International transfers of personal data for health research following Schrems II: a problem in need of a solution" <https://www.nature.com/articles/s41431-021-00893-y>

The war in Ukraine and the value of resilience

The Ukrainian Government's shift from data localisation to partner-nation headquartered cloud computing in the wake of the Russian invasion in 2022 is a clear example of the value of cloud computing and data flows as it essentially ensured the survival of the government's (digital) operations.²⁸ In this example, Ukraine moved large amounts of critical data to partner nation-headquartered cloud computing services, to ensure the resilience of data like the population register, land and property ownership, tax payment records, and education records. The Ukrainian Minister for Digital Transformation, Mykhailo Fedorov, stated, "the solution to save Ukrainian databases and state registers was cloud migration. What we like the most about this partnership with cloud companies is that Russian missiles can't destroy the cloud."²⁹ This was the last piece of legislation changed before the Russian invasion, as Ukraine had previously employed data localisation. Although the Ukraine situation is a severe case, it more generally demonstrates how international data transfers are important to resilience, whether to war, disaster, pandemic, outages, or other circumstances.

Cybersecurity

Data localisation undermines best-in-class cybersecurity, while data flows support it. Cloud and cybersecurity firms need seamless data flows to both share information to map global threat patterns against domestic ones or trace signs of malicious activity from global networks onto domestic ones. They also need data flows to take preventative and remedial action in the event of cyber-attacks. In the first systematic analysis of data localisation's impact on cybersecurity, Peter Swire and DeBrae Kennedy-Mayo show localisation prevents the sharing of cybersecurity-related information and that it undermines 13 of the 14 controls in one of the main international standards for information and cybersecurity (ISO/IEC 27002).³⁰ It also prevents local organisations from accessing best-in-class cybersecurity services. If firms lose the ability to collect and share security telemetry from around the world, it will be far more challenging to respond to cyber threats and attacks.³¹

²⁸ <https://www.nextgov.com/cxo-briefing/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/>

²⁹ *ibid*

³⁰ [The Effects of Data Localization on Cybersecurity by Peter Swire, DeBrae Kennedy-Mayo](#)

³¹ *ibid*

EU-US Data Flows

Whilst this Report examines the economic and social value in international data transfers, it has also emphasised that those transfers must be trusted. The Schrems I and II decisions³² from the Court of Justice of the European Union (CJEU) invalidated previous arrangements for international data transfers from the EU to participating organisations in the United States (the Safe Harbor Principles in Schrems I (2015) and Privacy Shield in Schrems II (2020)) on the basis of the US Government's ability to access, for surveillance purposes, personal data emanating from the EU, without appropriate legal constraints and satisfactory legal recourse for data subjects. More recently, the Data Protection Commission Ireland (DPCI) imposed a record fine of 1.2 billion EUR on Meta Ireland³³ in relation to the company's transfers of data from the EU to the United States post-Schrems II, in breach of Article 46 EU GDPR.

After the invalidation of Privacy Shield, Meta, the parent company of Facebook and Instagram, had relied upon SCCs and additional supplementary measures as the legal mechanism to transfer personal data to the US. However, according to the DPCI, the additional supplementary measures adopted by Meta "did not address the risks to the fundamental rights and freedoms of data subjects".³⁴ In essence, the DPCI (implementing the European Data Protection Board's decision to that effect) held that Meta had not taken (and could not take) sufficient measures to address the US Government's rights of access to users' data and thus the transfer of EU users' personal data to the United States should be suspended, with a deadline of five months for the suspension to be carried out. Meta described the fine as "a dangerous precedent" and that, "without the ability to transfer data across borders, the internet risks being carved up into national and regional silos".³⁵ Meta is appealing the DPCI's decision.

Such investigations and decisions by Data Protection Authorities act as a reminder that data access in the government sphere has a significant impact on international data transfers and trust in commercial actors more generally. They also emphasise the lack of legal certainty and the existence of an apparent conflict of laws, neither of which is conducive for trusted data flows. Companies alone cannot solve the challenges created by divergences in approach to protection against government access in different countries. The DPCI's decision in the Meta investigation is but one of several examples that clearly demonstrates the fundamental need for trusted government access to data, which will be discussed in greater detail in the next section of this Report. The decision may also have accelerated developments to facilitate international data transfers to the United States based on the newly agreed EU-US Data Privacy Framework, with an adequacy decision adopted by the EU Commission on 10 July 2023.



"Data access in the government sphere has a significant impact on international data transfers and trust in commercial actors more generally"

³² See <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362> and <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155>

³³ [Data Protection Commission announces conclusion of inquiry into Meta Ireland | 22/05/2023 | Data Protection Commission](#)

³⁴ *Ibid*

³⁵ [Meta hit with record \\$1.3 bln fine over data transfers | Reuters](#)

Of interest is the big discrepancy in the estimated volume of data flows outside the EU compared to the volume of data flows legitimised using recognised data transfer tools.³⁶ Findings from the UKBDS show 39% of businesses that send personal data outside the UK state they use no recognised legal safeguard (including data bridges or adequacy) to transfer personal data outside the UK.³⁷ Given the likely volumes of transfers, compared with the relatively low use of transfer tools reported in the surveys, it seems that most transfers take place without using recognised tools, with impunity, whilst major players using safeguards become the focus of decisions such as the DPCI's.

Key findings

The Council meetings and experts' written responses should continue to inform the Government's evidence and analysis agenda. For example, some members on the Council highlighted to DSIT reports by ITIF³⁸ on how to maximise innovation and productivity through new approaches to international data transfers, and on the impacts of potential new standard data protection clauses. While much of the evidence they shared was known to DSIT officials, getting perspective and insight alongside it from stakeholders in various sectors was highly valuable. These suggestions are in the process of being explored and actioned by UK Government analysts, who are, for example, building out modelling capabilities to better assess the economic impacts of data flow openness. Through highlighting work taking place internationally, experts suggested future analysis that could be interesting for the UK to explore. Examples included the US-based Bureau of Economic Analysis's (BEA) effort to value the US data economy³⁹ and the EU's studies on intra-EU flows and the cloud.⁴⁰ In turn, the Council will be making connections with relevant foreign government officials to consider this further.

The UK needs to ensure that it identifies and uses best practices in measuring the role and value of data flows and UK initiatives. Council members provided examples of current best practices on statistical measures, case studies and surveys to lay the ground on future work. The UKBDS mirrors some of the work undertaken by the BEA. How digitally enabled services are defined and how data transfers and used are broken down by size and sector. The UKBDS could be expanded upon with an understanding of BEA's best practice. Similarly, Japan undertakes related analysis including surveys that specifically ask businesses and organisations



“The UK needs to ensure that it identifies and uses best practices in measuring the role and value of data flows and UK initiatives”

³⁶ W. Kuan Hon, [Data Localization Laws and Policy](#), Edward Elgar Publishing (2017), Chapter 6

³⁷ <https://www.gov.uk/government/statistics/uk-business-data-survey-2022/uk-business-data-survey-2022--2#summary>

³⁸ [The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade | ITIF, Principles and Policies for “Data Free Flow With Trust” | ITIF \(2019\)](#)

³⁹ [Valuing the U.S. Data Economy Using Machine Learning and Online Job Postings](#)

⁴⁰ <https://digital-strategy.ec.europa.eu/en/policies/european-data-flow-monitoring>, <https://digital-strategy.ec.europa.eu/en/library/economic-value-data-flows> and <https://digital-strategy.ec.europa.eu/en/library/study-mapping-data-flows>

how they manage transferring data to multiple jurisdictions.⁴¹ UKBDS should consider such approaches to gain a better understanding of UK practices and issues involved in multi-jurisdictional transfers and to refine measures of the impact of UK data bridges and other agreements/initiatives. It points to the critical need for new and novel evidence to support UK digital policy and its overall vision for the global digital economy. First-hand accounts, aside from case studies, will add greater substance to evidence presented in relation to data flows. For example, carrying out interviews with UK businesses and organisations that transfer data to priority international data transfer countries will help better understand the potential benefits. To provide useful evidence of behaviour change and demonstrate the value of agreements, follow-up interviews should be undertaken to assess savings to organisations, as well as investigating changes to international data transfers methods.

Organisations want effective and efficient legal mechanisms rather than those that entail a large administrative burden while having little actual perceived impact on data protection practices. For organisations that transfer data as part of their normal day-to-day business operations, compliance with data privacy and security requirements is key to building trust. The application of high standards will bring about reassurance for both organisations and customers. Where there is no UK data bridge agreement, organisations will largely carry out international data transfers from the UK using SCCs. Also, many organisations that utilise BCRs report the commercial and trust benefits as their business customers perceive them as BCR-approved and accountable organisations with a high level of privacy and security protection. However, both SCCs and BCRs entail administrative and legal burdens and in the latter case, a protracted approval process in the UK and in the EU.

It is important to view data flows and privacy as elements that work together, rather than as a trade-off. Data flows are often discussed in terms of potential risk. **The narrative on data flows should be rebalanced - focusing not just on risk, but also on the benefits of building mutual recognition**⁴² and transfer solutions which work across multiple jurisdictions. The UK's aim of building interoperability would be a more tenable approach than championing full harmonisation. The Council believes accountability should be the principle at the heart of a global framework for responsible and trusted international data transfers. In order to achieve accountability and interoperability, policymakers should focus on ensuring that there is adequate protection of data wherever data travels. Countries should hold organisations accountable for how they manage their data, regardless of where they store it or process it.



“The narrative on data flows should be rebalanced – focusing not just on risk, but also on the benefits of building mutual recognition”

⁴¹ Eiichi Tomiura, Banri Ito, and Byeongwoo Kang, “Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms” (Research Institute of Economy, Trade and Industry, November, 2019), <https://www.rieti.go.jp/jp/publications/dp/19e088.pdf>

⁴² Such as the EU/ASEAN development, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

An international framework that potentially represents something significant is the Global CBPR Framework, as a broader multilateral evolution of the APEC Privacy Framework. When thinking about whether other international frameworks should be leveraged, there may be a limited number of alternative options that would make a significant difference outside of the SCCs and BCRs. However, CBPR could enable a global shift. Its system creates chains of accountability across digital settings and legal systems. It does not restrict international data transfers based on member laws nor does it require transfers to countries with APEC-compliant laws. The CBPR Forum believes its system is more accessible than other frameworks, making the CBPR privacy certification a good baseline solution for responsible data users. However, it would need to be amended to make it more interoperable with other legal frameworks such as the EU GDPR. CBPR could represent a scalable multilateral privacy assurance model likely to be of interest to a number of countries and, as such, the Council has focused Recommendation 7 on the potential of the Global CBPR.

Ascertaining the costs of transfer tools falls into two distinct areas: one which is easy to measure and one where the impacts are not necessarily measurable. There are some types of international data transfer tools where the economic cost of friction in data flows can easily be measured, such as the cost of transfer risk assessments, the cost of using BCRs or SCCs, the cost of receiving or providing worse (or no) services, and the cost of obtaining (or inability to obtain) access to services because of concerns over whether the destination country provides a reasonable level of data protection. Conversely, other types of impacts cannot or have not been costed, such as the exchange of information or medical research, safeguarding, and investigating tax avoidance or fraud. **The UKBDS could offer a wider platform for understanding the frictions related to data flows including support staff required, IT services, lawyers and ascertaining the resources involved.** This may present an indication on cost of transfer tools but also potential savings once a particular jurisdiction has a bilateral agreement with the UK. Updating the evidence base and surveys could provide valuable information on the role and impact of new UK data bridge agreements and transfer tools.



“Updating the evidence base and surveys could provide valuable information on the role and impact of new UK data bridge agreements and transfer tools.”

TRUSTED GOVERNMENT ACCESS TO DATA



The importance of trust in government access to data



Building on the OECD TGA Principles



Future initiatives



Differences in cultural and legal approaches to government access to data



Key findings

The importance of trust in government access to data

The issue of government collection, access to and use of data for the purpose of national security, intelligence, surveillance and law enforcement is a crucial one from numerous perspectives. For individual citizens who value their rights, and the civil society groups who represent them on their behalf, there is a desire for clarity regarding when and how government agencies may seek access to personal data for these goals.⁴³ For national security and law enforcement agencies, it is essential that they can access the information they need to operate effectively and to keep people safe. In industry, organisations have repeatedly made the case that, without certainty that international partners agree sufficient protections are in place and the regime governing government access to personal data is stable, they may be reluctant to allow certain international data transfers to take place.⁴⁴ This has the potential to cause significant economic damage and disruption, which makes increasing confidence in global government access regimes a crucial strand of work. In order to chart some potential next steps, the Council has sought to set out the current international state of play, proffer some ideas on how to promote the



“Government requests for data are increasing and, while governments have to comply with privacy laws in their respective jurisdictions, more evidence of accountability in this area would help to increase trust in international data transfers”

⁴³ The Council noted that the UK’s Data Protection Act 2018 covers law enforcement processing (Part 3) and intelligence services processing (Part 4), being one of the few countries to have placed the use of personal data for national security purposes on a statutory footing with a push for transparency.

⁴⁴ Eiichi Tomiura, Banri Ito, and Byeongwoo Kang, “Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms” (Research Institute of Economy, Trade and Industry, November, 2019), <https://www.rieti.go.jp/jp/publications/dp/19e088.pdf>

benefits of what has already been achieved and suggest actions that may encourage greater global cooperation on this issue.

In considering the range and breadth of requirements for government access to data, the Council is of the view that it is not possible to treat national security and law enforcement issues separately from wider data flows. Schrems I and II are clear indications that flows of commercial and scientific data have been restricted precisely because data could (irrespective of the actual likelihood) ultimately be accessed for national security and law enforcement purposes at a later date. Therefore, attempting to deal with national security and law enforcement access 'in silo' is not an option.

Building on the OECD's Trusted Government Access to Data Principles



TGA Principles

Legal basis

Access by government entities must be provided for and governed by the country's legal framework, enacted by democratically elected institutions operating under the rule of law.

Legitimate aims

The purposes of government access must be for specific and legitimate aims, not be excessive in pursuit of those aims, and be necessary, proportionate and reasonable with sufficient protections against abuse.

Approvals

There must be prior approval of government access, as detailed by law, with the stringency of requirements commensurate to the level of intrusion.

Data handling

Government access must be restricted to authorised personnel, with appropriate security measures in place.

Transparency

The legal framework for government access is clear and easily accessible by the public and enforcement bodies publicly report on government access.

Oversight

There are mechanisms for effective and independent oversight.

Redress

The legal framework provides individuals with effective judicial and non-judicial redress.

The Council observed that there appears to be a general lack of awareness or understanding about government access to data, including why governments need to access data, what data needs to be accessed, the controls and safeguards in place when handling data, the purposes and benefits of such data processing and with whom such data is shared (both nationally and internationally). Indeed, there is often a pervading sense of suspicion (whether founded, misunderstood or otherwise) on the issue. A major advancement was made by the OECD discussions on Trusted Government Access to Data, which, in December 2022, resulted in the Declaration on Government Access to Personal Data Held by Private Entities (TGA Principles).⁴⁵ The TGA Principles achieve two things:

- An important step in setting out when government access to data should be considered appropriate; and
- The establishment of a new cooperation mechanism that has brought together national security and law enforcement agencies to discuss safeguards concerning government access to data and domestic practices.

In reaching consensus on the TGA Principles, the OECD drew upon experts from diverse government actors with expertise in privacy, law enforcement, national security and economic affairs. These principles have properly considered the correct factors and utilised the appropriate expertise and should form the basis of wider global consensus on the topic.

While the OECD should rightly receive credit as the enabling forum to draw consensus and compromise for principles of an unprecedented nature, it remains regarded by non-members as overly exclusive to a small group of like-minded democracies. The OECD and its member countries should now focus on including nations from the 'rest of the world' if it is to best enable the wider dissemination of the TGA Principles and reap the benefits of raising global data standards. There is likely to be a balance to be struck between expanding the reach of the TGA Principles without suggesting every country is in a position to meet these standards.

Future initiatives

The Council discussed the benefits of working to incorporate the TGA Principles into a more binding arrangement or recognising those who adhere to them in some way that has tangible benefits for data flows or for organisations seeking to demonstrate that their adhering jurisdictions meet certain standards. The recommendations in this report are intended to promote the benefits of the advances that have already been achieved and facilitate greater multilateral cooperation through the expansion of the TGA Principles to the global arena. Possible future initiatives and actions are broken down into the categories below:

Political

To date, the OECD has developed the most mature model for trusted government access to data and has usefully set out the commonalities in member countries' approaches. However, given the limited representation (especially from Asia, Africa and South America), the UK should look to



“The recommendations in this report are intended to promote the benefits of the advances that have already been achieved and facilitate greater multilateral cooperation through the expansion of the TGA Principles to the global arena”

⁴⁵ <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>

reinforce and build upon the OECD's work in other multilateral political fora such as the G7, the G20 and the Institutional Arrangement for Partnership (IAP), as well as on a case-by-case basis with other individual countries. The inclusion of "Data Free Flow with Trust" in the TGA Principles is helpful given it is a concept that has already been raised in other fora. There is also a possibility to link with, refer to, or incorporate the TGA Principles into other multilateral mechanisms, such as the Global CBPR system, to address the inevitable concerns of how the CBPR countries address the issue of government access to data. Finally, it is also possible to conceive, in the medium-term, further work to implement the TGA Principles, to actually drive accountability of the government agencies when accessing and using data for national security purposes.⁴⁶

Regulators

Increased engagement between regulators would assist in furthering the progress of this work. Building and supporting mutual understanding, cooperation, strategic objectives, and approaches between regulators can help support the flow of data, address concerns and reduce unnecessary restrictions. Such work is already being conducted in a number of fora, including the Global Privacy Assembly (GPA), the group of G7 regulators, the OECD and elsewhere. However, more could be done to operationalise these discussions and produce tangible outputs that support "data free flow with trust". The GPA could be a practical forum to help facilitate this given its global reach and convening capability. However, while regulators can communicate, cooperate and agree on strategic objectives, it is up to governments, legislators and national security bodies to address specific differences in laws and practices which may give rise to varying regulatory approaches, and to liaise proactively and constructively with regulators to ensure that the nuances/practicalities of national security and law enforcement are taken fully into account.

Business

The business community has a big stake in this work and should articulate the importance of data flows for their sectors, customers, and stakeholders (e.g., through developing case studies to share with governments). This will help inform policy making and a broader public narrative, promoting the benefits of international data flows for society more generally. International bodies including the World Economic Forum and industry bodies could serve as appropriate communities in which to articulate the economic case, to complement the political and regulatory actions/initiatives mentioned above. In addition, businesses must continue to develop and implement accountable policies and procedures for dealing with government access to data in a way that ensures their and governmental accountability, protections for individuals, legal compliance, and transparency.



⁴⁶ [Privacy-Bridges-Paper-release-version.pdf \(huntonprivacyblog.com\)](#)

Differences in Cultural and Legal Approaches to Government Access to Data

Variance in cultural and legal approaches to government access to data is a reality that must be acknowledged and worked with, rather than against. Rather than seeking legal alignment or precise replication of words or processes (harmonisation), the UK should champion an approach that seeks to focus on shared objectives and similar outcomes (interoperability). This may involve engagement with countries whose national security regimes and data protection laws are under construction or require significant development. The UK should not shy away from this, even if prima facie it could prove more challenging than engagement with, for instance, OECD countries. Moving away from opacity or unwillingness to discuss national security and law enforcement issues internationally is a crucial step. More transparency through a willingness to discuss and engage will allow countries to make reasonable assessments and/or comparisons of the national security regimes elsewhere. Indeed, if this transparency extends (as much as is practical) to some sort of multilateral forum, that will make it easier to assess multiple countries' regimes simultaneously, to everyone's mutual benefit.

Examples of key differences in approach between different countries are:

- **Common law and civil law approaches** – particularly regarding the structure of criminal prosecutions, which varies considerably among nations. In some countries, an investigatory magistrate has broad powers to access data held in the private sector.⁴⁷ By contrast, in others, the common law tradition relies more heavily on investigatory officers first securing a warrant from a magistrate or other judicial officer. These differences need to be taken into consideration when evaluating similar objectives, rather than focusing on differences in process.
- **The institutional structure of governments** – while the UK and many other nations have a parliamentary system, countries such as the US have a presidential system. Legal rules and allocation of power thus may differ on the relationship between the legislature and executive. Such differences can affect the governance of national security and data collected for national security purposes. In a parliamentary system, fundamental decisions on national security rely on continued support from the legislature. In a presidential system, the president may have significant scope for action on national security matters, separate from the need for continued legislative support.
- **The nature of constitutions** – this varies considerably between nations, sometimes with specific provisions that lead to different institutional arrangements for government access to data for national security and law enforcement purposes. The process of developing the TGA Principles by the OECD showed that there are indeed important differences in the domestic legal systems of government access to data, both in the law enforcement and in the national security fields. Still, different legal mechanisms could sometimes achieve the same objectives and could, depending on the circumstances, offer strong human rights protections. Examples are the mechanisms in place



“Rather than seeking legal alignment or precise replication of words or processes (harmonisation), the UK should champion an approach that seeks to focus on shared objectives and similar outcomes (interoperability)”

⁴⁷ Peter Swire, Justin D. Hemmings, and Suzanne Vergnolle, “A Mutual Legal Assistance Case Study: The United States and France,” 34 Wisconsin International Law Journal 323 (2017).

between the United States and the UK, including the US Executive Order that addressed the concerns about Privacy Shield litigated in Schrems II and led to the Data Framework Privacy Agreement. The recent UK-US Data Access Agreement⁴⁸ also introduced a new process for UK law enforcement and intelligence agencies to obtain content data from US-based communication service providers, to combat the prejudice to investigations that was caused by delays in the UK/US Mutual Legal Assistance Treaty process. As this process matures, learnings from it will be of considerable value.

In light of national differences in criminal investigations, the institutional structure of government and constitutions, there can be variations in the precise institutional mechanisms for governing government access to data held by the private sector. These variations are an important reason to support and expect international convergence based on principles for government access, rather than insisting on precise replication of one country's institutions for such access.

There may be some utility in engaging some independent intelligence oversight bodies to discuss and develop potential solutions and approaches to government access to data. These bodies (e.g., Investigatory Powers Commissioner's Office) work transparently and will likely have been posed similar questions. It would be of value to engage them (including international bodies and bodies in other jurisdictions) on these questions, which will allow any solutions to be underpinned by relevant experience and good practice.

There could be potential to expand the scope of national security/law enforcement approaches to cover other forms of government requests for data sharing, for example, to include ad hoc access to data sent to the government by various sectors in aid of the general functioning of the government, access by the government to commercially available data, publicly available data or data voluntarily provided by the private sector to the government. Government requests for data are increasing and, while governments have to comply with privacy laws in their respective jurisdictions, more evidence of accountability in this area would help to increase trust in international data transfers. This is a global issue that would benefit from focus and constructive engagement.



“There could be potential to expand the scope of national security/law enforcement approaches to cover other forms of government requests for data sharing”

Key findings

The work of the OECD on trusted government access to data, including the TGA Principles, should be referenced, leveraged and/or extended to other multilateral fora, such as the G20, the Global CBPR System, as well as bilateral arrangements between OECD and other countries.

Increased engagement is needed and should be facilitated between different countries' national data protection regulators (e.g., through the Global Privacy Assembly), the national security and law enforcement

⁴⁸UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019] - <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-counterinq-serious-crime-cs-usa-no62019>

community, and lawmakers in respect of access to data for national security and law enforcement purposes.

The views of the business community, civil society, and intelligence oversight bodies are extremely important in shaping agreed principles for trusted government access to data.

While government access to data for national security and law enforcement purposes has been a specific focus, **greater awareness of the requirements of government to access data for the proper functioning of government** (e.g., to understand and address local and global issues such as ESG, health, space, and ocean-related international issues) and to support citizens, is needed.

Gathering learnings from the operation of the UK-US Data Access Agreement, as to access to personal data on an international basis by law enforcement, will be of huge value.

UK GOVERNMENT TACTICS AND STRATEGY FOR ACHIEVING ITS GOALS



The UK as a safe data hub promoting trusted international data transfers



The impact of data localisation



The UK's role in international data transfer policy



Strategies and tactics



Developing and advocating its vision for international data transfers



Key findings

The UK as a safe data hub promoting trusted international data transfers

With due regard for its independence from the UK Government, the UK must support domestically and internationally the work and role of the Information Commissioner's Office (ICO) as an ambassador of the pragmatic, yet robust, approach to data protection and international data transfers compliance, interpretation and oversight. The ICO is considered a modern, effective, risk-based and transparent regulator that is influential in global privacy law, policy, and practice, with a progressive regulatory strategy, innovative initiatives and helpful guidance that seeks to ensure robust protection for individuals while promoting responsible and accountable use of data for the benefit of all (individuals, society, and organisations). Given the influence of the ICO in the global data protection community, and the pragmatic governmental data and digital policy, the UK is in a strong position to facilitate bridge-building towards interoperable international data transfer arrangements. The UK is also a hub of international data transfers and one of the countries seeking to expand its economy upon the liberalisation of trade and "data free flows with trust."



"Given the influence of the ICO in the global data protection community, and the pragmatic governmental data and digital policy, the UK is in a strong position to facilitate bridge-building towards interoperable international data transfer arrangements"

The UK and its partners would benefit greatly from the removal of barriers to international data transfers throughout the globe, but this is only possible if data transfers are trusted and secure. The requisite protection of data can be achieved by establishing and applying a set of agreed standards that will be followed across jurisdictions, meaning that data is safe irrespective of where it flows to.

This section of the Report sets out the Council's view on the UK's role in the development of interoperable arrangements for international data transfers as an independent actor, how a narrative ought to be developed to support its policies and goals, followed by a discussion of both short-term tactics, to be carried out over the next two years, and longer-term strategy, toward the UK being a safe hub of trusted international data transfers.

The impact of data localisation

Data localisation is increasingly presented as a solution to data protection and other challenges, due to the belief that, when data is stored within the locality in which it was created, it is better protected. As the remainder of this section will set out, this belief is mistaken. Having effective jurisdiction over those who control access to data, and how well they secure that data, matters more in practice.

The UK should continue to push back against the pervasive and growing narrative that localisation is a system that can be used to better protect data. Measures are often put in place under the banner of security or data protection⁴⁹ but, in reality, they are often used for economic and political reasons. This may include ensuring access to data of their citizens for political surveillance purposes or a country's desire to ensure they can retain ongoing access to the data of their residents and businesses operating within its borders. Often, data localisation policies are hallmarks of jurisdictions which themselves have fewer protections for personal data. However, this is not always the case. In other instances, it is not authoritarian purposes but efforts to promote the development and growth of local businesses, particularly in the technology sector, that result in de facto localisation.

The availability of remote access and encryption have broken pre-Internet notions of a one-to-one correspondence between intelligible access and data's physical location.⁵⁰ Data localisation is also entirely at odds with today's global society, which has relied on the development of Internet-based communications and services to progress in a way that is essentially irreversible and incompatible with geographically ringfencing data. Organisations of all sizes routinely transfer data automatically across borders. As servers in one country or region become overloaded, they may automatically transfer processes and often data to another, located in another region or country. All of this will be done in seconds without the user noticing or the system recording these movements.

However, there are good reasons why international data transfers can be safer than data localisation. Indeed, non-localised data storage is one of the best



“Data localisation is also entirely at odds with today's global society, which has relied on the development of Internet-based communications and services to progress in a way that is essentially irreversible and incompatible with geographically ringfencing data”

⁴⁹ “The Extent and Impact of Data Localisation: Report prepared for DCMS”, 1 June 2022, [Frhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf)

⁵⁰ W. Kuan Hon, *Data Localization Laws and Policy*, Edward Elgar Publishing (2017) and [see](#) above, at footnote 32

protections for data availability against natural disasters affecting a geographic area.⁵¹ Data that is allowed to flow freely can be moved from a system or a server that is compromised. It will be stored in multiple places and simply leave behind a redundant system or server. This will support availability, business continuity and resilience in a time of crisis (see, for example, the case study about Ukraine on page 15). Conversely, localisation can leave data and often whole systems under serious threat by siloing their security systems in limited geographic locations. A single standalone server will not have as strong protections as a system that can be updated and learn from global threats. The best way to ensure the privacy and security of data is to establish a set of baseline principles that will be followed in all jurisdictions, so – no matter where the data flows – it will be secure, private and responsibly used.

Moreover, data localisation is extremely difficult if not impossible to implement in practice, as today's digital services require access to that data globally. The digital world does not recognise geographic boundaries. Even data localised in a specific jurisdiction or region can be accessed remotely by governments overseas, including by US law enforcement, when global organisations operating in that jurisdiction or region operate with a base in the US.⁵² As one member of the Council said, “employing data localisation is like trying to put toothpaste back in the tube”.

The case against localisation is further supported by economic arguments. The way to gain benefit from data is to use it. Combining and using data and applying new ways of thinking is the only way to extract the greatest value from data. If data is allowed to flow via responsible, trusted and accountable international data transfers, it supports trade and encourages business connections and freedom of expression/information - data has no value when locked away. This is particularly true in the case of AI and the increased national and global focus on broader and faster adoption of AI, the development and use of responsible AI technologies, and the promotion of countries' AI based industrial policies. For AI and machine learning technologies to be responsibly developed and deployed, they require vast amounts of data, from different sources and locations, and with different diversity factors. These are necessary prerequisites for training of algorithms and foundation models to ensure their fairness, non-discrimination, accuracy, safety and security. In brief, AI requires international data transfers so countries imposing data localisation requirements are impeding their own ability to grow and compete with their own AI capabilities.



⁵¹ Ibid.

⁵² <https://privacycrossborders.org/wp-content/uploads/2023/03/cipl-tis-discussion-paper-ii-data-localization-and-government-access-to-data-stored-abroad-march-2023.pdf> (privacycrossborders.org)

The UK's role in international data transfer policy

The UK already takes a prominent position in the global data arena as a country looking to liberalise both trade and data flows, while promoting trust, accountability and protection for personal data and rights of individuals. This is combined with the reputation of the ICO as its data protection regulator, which is a real asset to the UK in promoting its approach to data protection and international data transfers. It is crucial that the UK maintains consistent aims and an overarching vision across all of the multilateral fora it is engaged in. This must be coupled with presenting itself around the globe outside of the traditional multilateral fora, since expanding the scope of bilateral engagements is also essential. The focus should be on the global narrative of data protection, approaching countries directly; the UK being confident in its own narrative and vision for the future.

Working with international partners

It is important to acknowledge the contribution that the UK can make to international frameworks and institutions that may have a wider remit, but which may play a significant role in the development of global data protection practices. Many charities, civil society groups, standards agencies, trade bodies and respected global institutions will have an interest in the global data landscape even if it is not their *raison d'être*. These include organisations such as the International Standardisation Organisation (ISO), the World Economic Forum and Privacy International. Working with these institutions, often not directly associated with data, will help the UK build a base of support and a global narrative that suits its interests.

This approach will not return quick results but should be the basis of the longer-term strategy for the UK. Building broad support across all layers of government, business and civil society will lead to greater alignment of global dimensions that can lead to positive outcomes in this space. Engagement is key.

Expansion of the network to high growth countries

The UK should engage with high-growth countries both through international fora, but also on a bilateral basis where appropriate (in terms of the time and resource commitment involved), with a view to facilitating trusted international data transfers with the UK. Engagement with these countries should have the goal of developing data protection regimes that are suitable for a UK data bridge and capacity-building. It would be essential to ensure that the relationship is a partnership of equals or agreed to under the banner of increased global trade⁵³ alongside developing a sustainable and future-proof data protection regime.

The UK could offer advice and support to government officials working on privacy and data protection policy and delivery in high-growth countries. For example, there are already examples of partner countries engaging with the expertise of the ICO.



“It is crucial that the UK maintains consistent aims and an overarching vision across all of the multilateral fora it is engaged in”



<https://www.oecd-ilibrary.org/trade/mapping-commonalities-in-regulatory-approaches-to-cross-border-data-transfers/ca9f974e-en>

UK-EU Relations

Following Brexit, the UK-EU relationship is evolving. Both the UK and the EU will continue to face common geopolitical and geo-economic challenges and the UK and EU have an important stake in the continuing stability of their data relationship. Although the EU-UK adequacy decision is good for the UK, it is also beneficial for the EU and essential to many EU businesses. The relationship is not simply one-way, so it is important that the UK and EU maintain a constructive relationship based on mutual respect and shared interests.

The UK's global position relative to the EU is critical. Before Brexit, the UK contributed to European data protection legislation in a pragmatic and progressive way. The UK could continue to play an influential role by engaging in a proactive and open way with the EU, exchanging views and sharing its vision in a constructive and complementary manner, especially in the context of further developments under GDPR, related digital regulation and AI. However, it is important to note the increasing trend of digital sovereignty across the EU which has the aim of providing a boost to EU industry and capabilities in emerging technologies as well as reducing EU dependence on non-EU actors. The UK will need to engage with the EU and member states to ensure this does not adversely impact data flows. This ongoing dialogue with the EU can continue alongside building relationships with regulators and individual government agencies within countries that may be warmer to the UK's global approach to data. Building these connections coupled with expanding the UK's relationships outside of the major data fora will help spread and build support for the UK's long-term vision for data, within and outside of Europe.

A constructive UK-EU relationship on data is essential in projecting confidence in global cross-border data flows. Internationally, the UK is establishing itself as a global leader in the data space and, by working together with the EU as appropriate and emphasising the shared legacy, both the UK and the EU can maximise the opportunities presented by international data transfers between them and other countries which are regarded as adequate by the EU and with which the UK has established a data bridge. As such, the EU is a critical international partner with whom the UK needs to engage and to build a good working relationship.

To achieve this the UK must position itself as a partner of the EU, with many shared common interests and goals. While the UK will engage as an independent actor, it should involve the EU as a close partner in its global vision of interoperability. This approach will provide the greatest levels of stability for organisations and will reaffirm the robustness of the levels of data protection in the UK.

Strategies and tactics

The UK's international goals are simple: establishing itself as a data leader and building towards an interoperable global system of trusted, accountable, and responsible international data transfers. However, these goals become challenging to reach in a fractured landscape. The UK is scaling up its work to secure bilateral agreements on international data transfers with priority partners across the world and is investing in opportunities to design globally interoperable transfer mechanisms with international stakeholders from the OECD, the G7, the Global CBPR Forum and the Council of Europe. These are solid bases from which to build the wider network of stakeholders mentioned above.



“Although the EU-UK adequacy decision is good for the UK, it is also beneficial for the EU and essential to many EU businesses”



One of the first practical steps the UK must take to start building an international system is to address the issues exposed by the CJEU's Schrems II ruling,⁵⁴ in particular the need for organisations to assess the powers of public authorities in other jurisdictions to access personal data transferred from Europe. Overcoming these issues is a very complicated element of the current GDPR framework but the UK and its partners are well placed to contribute to a solution.

Although some organisations are following the requirement to conduct a transfer impact assessment⁵⁵ before international data transfers, established by Schrems II, many are not realistically able to do so. This has led to an unlevel playing field for business. A key step towards building a cooperative international system is to standardise and make transatlantic international data transfers, critical for the UK economy, easier for all UK businesses, especially small and medium-sized enterprises. If compliance becomes too burdensome, many organisations simply will not do it. Those who comply are incurring costs, whereas those who do not comply are transferring personal data internationally with impunity. This does not make international data transfers safer or more trusted. This situation could be improved by establishing a UK-US data bridge for international data transfers, as heralded in the Atlantic Declaration. This is particularly important as the European Commission has now adopted an adequacy decision for the United States in the EU-US Data Privacy Framework.⁵⁶ The UK cannot be left behind in this critical data market.

Quick-wins

Instead of opening up a new broad scale of programmes to expand the UK's global data effort, outside of increased engagement it would be more effective in the short-term to support projects already in existence. DSIT could build upon projects led by the Foreign, Commonwealth and Development Office and United Nations Conference on Trade and Development by introducing aspects of data governance to help build capacity and skills within the country, focused on digital capacity, and help facilitate UK data bridge decisions for those countries in the longer term.

This would, in the short-term, allow the UK to actively engage with a series of stakeholders operating outside the more traditional EU and US spheres of influence that would likely be receptive to the UK's vision for data governance, on the global stage. It would also provide the baseline for a longer term 'win' by helping to build a data protection regime that would succeed in a UK data bridge assessment or be more closely aligned to join an interoperable multilateral framework. The key to the UK's 'quick wins' is broad engagement. At any forum where data is to be discussed, the UK needs to be present with its well-argued baseline vision of the future of international data transfers.



⁵⁴ See page 16

⁵⁵ Also known as a Transfer Risk Assessment in the UK

⁵⁶ [Adequacy decision for the EU-US Data Privacy Framework | European Commission \(europa.eu\)](#)

Developing and advocating its vision for international data transfers

It is important that the UK communicates a clear and consistent narrative across all platforms to ensure that its views are well understood and accepted. This UK narrative should consist of:

- Support from leading UK organisations who provide services in the areas in which the UK is historically strong. Countries must have a reason to care about international data transfers to and from the UK and the UK must be conscious of the need to transfer personal data outside of the UK for services to be provided to UK organisations.
- Building engagement with charities and other non-governmental bodies who recognise that removing barriers to international data transfers creates benefits and opportunities, both domestic and global. This could be in areas such as combating climate change, new pandemic challenges, or keeping children safe online.
- A commitment from the UK to place greater emphasis on increasing the security of the data wherever it is located, whether technical or organisational. Even if data is localised, if it is on badly protected vulnerable equipment or lacks proper access controls, then it is open to nefarious actors, irrespective of the laws in place. Security is paramount, whether data is at rest or in transfer.
- A wider push from the UK based on evidence that increasing localisation actually leads to increasingly unsafe storage (reducing backups to other geographic locations in case of natural disasters) and lost opportunities.
- The need to engage society, business, government and third sector benefits and opportunities of trusted data flows.

The narrative must be backed up by a plan and a set of measurable goals to demonstrate its effectiveness. Further, the UK's narrative should be disseminated around the globe by providing support to other countries to build their own data protection regimes, which will build data skills and capacity within these countries. This could be done through organisations like the BSI, on an ad hoc basis, by working together with public officials, by international engagement via the ICO, or through a trade deal.

The process of disseminating the narrative will not be quick and it will take time to develop those deeper relationships. This will, however, provide a solid base of support for years to come both domestically and globally for the UK's goal of a global framework for international data transfers. The creation of a UK narrative to all other nations should be coupled with a narrative to the UK public to build grassroots support for the UK's ambition.

The UK's narrative should focus on the benefits of data transfers to the economy, society and individuals' lives. Three key examples that the UK should support are (1) civil society groups that promote children's safety and encourage the international data transfers where it helps to protect children online, including content moderation requirements, (2) cybersecurity, where international data transfers are critical for cloud providers, other organisations, and critical infrastructure organisations to protect and defend against cyberattacks by ensuring the security and integrity of their systems and data,



“The UK’s narrative should focus on the benefits of data transfers to the economy, society, and individuals’ lives”

and (3) AI algorithmic training and applications that use data in a fair and non-discriminatory manner.

The UK must build support for its messaging on international data transfers by finding like-minded partners. This public narrative on transfers should be coupled with messaging that promotes how fundamental the security of data architecture, and organisational security policies, are to overall data security and privacy, and the importance of technical and not just contractual or organisational measures for protecting data.

Key findings

Data localisation is extremely difficult, and in practice unviable, in a digital world that does not recognise geographical boundaries. Therefore, international data transfers should be seen as a much-needed reality for the world to function and prosper. The UK should make its public narrative on international data transfers bolder as to the wider benefits of international data transfers to the economy, society and individuals' lives and should use it consistently, both domestically and internationally.

The UK should continue to deepen its relationships with existing international partners while supporting new partnerships to facilitate the delivery of its own and its partners' international data transfer policies. The UK should look to establish a data bridge with key partners to improve the ability to carry out international data transfers and level the playing field, as well as promote and monitor trusted, accountable and responsible international data transfers to and from high-growth countries.

The EU remains a strategic partner with the UK. **The UK and EU should continue their collaboration on data and data transfer issues and face the common challenges in a spirit of cooperation and partnership.**

The UK could leverage its "rich" data assets (both hard quantitative data sets provided by bodies such as the Office for National Statistics and soft qualitative data assets provided by interpretations of data) to **expand its support for digital capacity-building and the adoption of improved data governance standards in high-growth countries in need of such support.** The UK should continue to dedicate resources to solving challenges surrounding international data flows, including through evidence-based policy making.

The UK should increase engagement with civil society groups, standards bodies, and NGOs in the design and delivery of its international data transfer policies. It needs to move beyond the major international players to build support for the UK's message in all sectors and fields. Data is essential for all activities in the modern economy.



“The UK should continue to deepen its relationships with existing international partners while supporting new partnerships to facilitate the delivery of its own and its partners' international data transfer policies”

MULTILATERAL SOLUTIONS FOR SUSTAINABLE AND SCALABLE INTERNATIONAL DATA TRANSFERS



Beyond bilateralism



Considerations on delivery of the ideal system of international data transfers



Toward commonly accepted standards



Multilateral fora



Regulation and enforcement on a global scale



Key findings

Beyond bilateralism

The introduction to this Report explained why trust is crucial to removing barriers to international data transfers. To produce the requisite trust in international data transfers, most countries that restrict international data transfers regulate through the adoption of unilateral, bilateral or regional measures that rely upon reciprocity and extraterritorial reach, as well as various data transfer mechanisms. Inevitably, the measures vary between different jurisdictions. For various reasons, the consequent patchwork of domestic and bilateral instruments is not conducive to a sustainable and scalable global system of trusted, accountable and responsible international data transfers. There is a danger that the world is headed on a trajectory towards a “data



“The consequent patchwork of domestic and bilateral instruments is not conducive to a sustainable and scalable global system of trusted, accountable and responsible international data transfers”

blocs” scenario of increased fragmentation, with declining multilateralism, and diverging standards.⁵⁷

A natural response to the above barriers is that organisations may limit the extent to which they transfer data beyond jurisdictional confines or may transfer data in a way non-compliant with any restrictions on international data transfers. This situation reduces the benefits of international data transfers for citizens, as well as for private and public sector organisations. It also harms the digital economy and societal progress, as well as opportunities for technological and policy innovations.

The above challenges are largely created by the restrictions themselves: the fragmented nature of bilateral and regional approaches being taken throughout the world (i.e., establishing data bridges one-by-one). These cannot be scaled up globally. This is then combined with rigid interpretation of the law by some regulators and consequent implementation of more restrictive data flows by organisations. For example, some cloud providers are now incurring costs (which may be passed on to customers) to offer localised services where data will be confined to servers in one region, because organisations are finding it too burdensome to transfer personal data internationally and understand the complexities around international data transfers. Resolving these issues cannot be the result of purely siloed domestic reforms. Rather, the solution may be in the form of effective multilateral arrangements that recognise data protection and privacy as a matter of human rights.

Therefore, the Council has considered what could be done to improve the current outlook. Specifically, it looked at what multilateral arrangements could be utilised, what could be learned from multilateral fora working in other policy fields, what specific initiatives should be prioritised and whether a new international body or agreement is necessary.

Considerations on delivery of the ideal system of international data transfers

To achieve the ideal system of international data transfers the Council recommends an approach to engagement on data (more broadly) and “data free flows with trust” (more specifically) with multilateral institutions and multilateral frameworks. This means engagement with specialised multilateral fora and frameworks, with some better suited for political commitments, and others for more granular work. Such an ideal international data transfer system could be delivered by:

- **Engaging with multiple multilateral fora** - The current multilateral landscape is characterised by an abundance of international fora that only tangentially or only partially consider all the aspects of data. These all seek to make positive contributions to a more functional data ecosystem with data governance through principles, guidelines, or binding rules, but very few have successfully taken concrete action to fundamentally progress the data governance landscape. All are in some way limited, for example, due to a lack of global reach or lack of



“The current multilateral landscape is characterised by an abundance of international fora that only tangentially or only partially consider all the aspects of data”

⁵⁷ See Information Technology & Innovation Foundation (ITIF) Report on “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them”, 19 July 2021, available at <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

consensus. Despite the limitations of existing multilateral fora, there should be engagement with and between all relevant fora to maximise the advocacy for trusted international data transfers and to not preclude fora that may later make a positive impact. Different approaches may be needed in different fora.

- **Learning from other policy areas** - There are lessons to be learnt from successful multilateral initiatives in other fields, such as finance and intellectual property. The world of intellectual property shows what a fully developed global system could look like, and the work of the Financial Stability Board shows what is possible when there is political will.
- **Continuing to harness bilateral relationships** - Multilateral engagement should not be prioritised at the expense of bilateral arrangements, which continue to be crucial and may often act as a catalyst for further multilateral advancements.
- **Prioritising Stakeholders** – The key stakeholders are first those which are committed to “data free flow with trust” (the G7 countries, the members of the OECD, and the Global CBPR Forum), followed by key UK partners and those with nascent data protection regimes.
- **Taking a multifaceted approach** – No single mechanism or forum should be prioritised. Rather, a variety of approaches should be taken, to reflect different types and natures of data flows, which can serve as building blocks towards a more interoperable global system.

Towards commonly accepted standards

International data transfers would be facilitated if common globally acceptable standards can be agreed, such as one based on the updated OECD Privacy Guidelines. The Council considers that the Global CBPR system is an interesting example that bridges the gaps between differing national privacy laws across participating jurisdictions and ensures that baseline common protections travel with data across jurisdictions. As such, it proves a useful model and foundation for the creation of a universal standard and a process for multilateral global certification that enables trusted data flows.

APEC was the first multilateral forum to host this system. Its core principles (Preventing Harm, Integrity of Personal Information, Security Safeguards, etc.) are translated into fifty CBPR programme requirements. Participating countries must demonstrate that CBPR programme requirements will be legally enforceable against certified companies, and certified companies must demonstrate to an Accountability Agent that they meet the CBPR programme requirements. The APEC CBPR system also encourages regulatory cooperation through the Cross-border Privacy Enforcement Arrangement (CPEA).⁵⁸

It is therefore a system which offers effective protection, enforceable standards, accountability, and regulatory cooperation. With the launch in April 2022 of the Global CBPR Forum,⁵⁹ there is an opportunity to contribute to the evolution of

⁵⁸ Information provided by the US Department of Commerce during engagement in September 2022.

⁵⁹ The Global CBPR Forum participants are Australia, Canada, Japan, the Republic of Korea, the Philippines, Singapore, Taiwan, and the USA.



“The Global CBPR system is an interesting example that bridges the gaps between differing national privacy laws across participating jurisdictions and ensures that baseline common protections travel with data across jurisdictions”

this system into the Global CBPR Framework that goes beyond the APEC member economies.

The APEC iteration of CBPR has had only a limited uptake from industry, for example when compared to participation in the EU-US Privacy Shield (before that was struck down by the CJEU). Other crucial partners, such as the EU, have been reluctant to seek bridges with APEC's CBPR.⁶⁰ The Global CBPR Framework presents new potential for an existing tried and tested system which could be improved and updated, where necessary, over time. As a globally acceptable privacy accountability mechanism, it was greatly influenced by the origins of the APEC Privacy Framework, but it does not have to be bound by the past. In fact, there has been significant change and legal developments since the adoption of APEC Privacy Framework, and it would be only natural to seek to upgrade the rules to reflect the developments in OECD guidelines, the GDPR, and other key privacy laws.

If the EU, the UK, the US, and other like-minded countries could agree on common standards, this would facilitate international data transfers, offering possibilities for growth and innovation. In order to do so, the key requirement would be to bridge the Global CBPR Framework, and the EU GDPR and the UK GDPR. Whilst there is currently a gap in standards between the EU and UK GDPRs on the one hand, and the CBPR on the other, there is complementarity between the two.⁶¹ There is scope to augment the CBPR standards to bridge the gap, for example by instituting a data breach notification requirement.

Mutual recognition bridges could be formalised, for example through recognising CBPR certifications as sufficient to enable international data transfers under, for example Art.46(2)(f) UK GDPR, to organisations that are certified. Binding commitments from those certified would also be required, and the UK could lead the way here, to propose a standardised approach to such commitment. If the UK were able to encourage the bridging of these gaps, it could ensure better and more accountable flows of personal data.

The UK should engage with the Global CBPR Forum which, unlike the APEC Forum that is restricted to the Asia-Pacific, is open to all countries. The Global CBPR Forum is still in its early days and would be ideal to facilitate broad engagement. It has the potential to evolve into a truly multilateral framework. The UK should seek to influence the governance and design of the Global CBPR system, by encouraging an upgrade of standards and/or programme requirements, so that they more closely track the recent developments in global data protection laws and bridge the gap with UK standards. The UK should build upon its associate status in the Global CBPR Forum, which provides a better position to engage and influence, and consider becoming a full member



⁶⁰ See Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act of the Protection of Personal Information, 2019 O.J. (C/2019/304) ¶ 79, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0419&qid=1689692284887>; see also Communication from the Commission to the European Parliament and the Council (2017) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN#footnoteref47> (suggesting work to explore convergence between BCR and CBPR, which has not been pursued since the European Commission made the statement in 2017).

⁶¹ Bojana Bellamy, Markus Heyder, and Sam Grogan, "APEC Cross-Border Privacy Rules Requirements and EU-U.S. Privacy Shield Requirements Mapped to the Provisions of the UK General Data Protection Regulation," CIPR, April 19, 2021, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_study_-_apec_cbpr_system_and_eu-us_privacy_shield_mapped_to_uk_gdpr.pdf.

of the Global CBPR Forum if and when standards and industry uptake reach a certain threshold.

Standards organisations could play a role in facilitating data transfers. The International Standards Organization is an NGO which develops international standards through which it is possible to certify.⁶² However, certification to ISO standards does not currently suffice to obtain UK or EU GDPR certification.⁶³ The common standards could come in the form of the ISO 27000 series⁶⁴ or other newly developed ISO standards linked specially to data transfers. The UK should scope out possibilities for recognising existing standards⁶⁵ under the Article 46(2)(f) certification mechanism in UK GDPR through engagement with the ICO. If this route does not prove feasible, work with industry bodies to develop new standards that can be recognised as certified and mutually recognised tools for international data transfers (such as standards on confidential computing/Trusted Execution Environments, homomorphic encryption and multi-party computation). Approved certification standards with built-in encryption, when mutually recognised, would have the advantage that importer-country government authorities could not have intelligible access to the personal data transferred. Whilst the process for developing a standard usually takes three years, the engagement with ISO should begin as early as possible, so that the standard development process can begin. Such an initiative emanating from ISO would have a wide reach (currently 167 member countries), but engagement with other standards organisations such as ETSI should also be encouraged.⁶⁶

While working on a sustainable and universal multilateral framework for trusted and responsible international data transfers, the UK must not lose sight of the short to medium term possibilities of evolving, mutualising, and expanding the existing transfer mechanisms, such as SCCs and BCRs:

- The UK should attempt to “multilateralise” SCCs and BCRs by agreeing their mutual recognition on a multilateral basis, and harmonise these tools to allow transfer mechanisms, especially SCCs and BCRs, to be employed across jurisdictions;
- This would be complemented by the recognition for transfers purposes of appropriate industry standard security certifications, suggested above, as tools for international data transfers. Such recognition could be achieved through using a third-party accreditation provider, commissioned by the ICO, which could be facilitated by using the ICO’s powers to charge for certain services.
- If BCRs can be made simpler, faster, and more cost-effective, they could be used by more than just the largest corporations. To support this, the ICO could consider AI-assisted review of BCRs for a streamlined and efficient process. This could, ultimately, lead to enabling international data transfers from one BCR-certified corporation to another BCR-certified corporation; and
- The UK could commission local law assessments for key countries that UK exporters can utilise in drafting Transfer Risk Assessments.

⁶² “About Us- ISO,” ISO, February 16, 2021, <https://www.iso.org/about-us.html>.

⁶³ ICO, “Certification FAQs,” ICO, January 26, 2023, <https://ico.org.uk/for-organisations/certification-faqs/>.

⁶⁴ “ISO/IEC 27001 and Related Standards,” ISO, October 25, 2022, <https://www.iso.org/isoiec-27001-information-security.html>.

⁶⁵ Such as the BSI data protection standard and security standards.

⁶⁶ “Standards, Mission, Vision, Direct Member Participation.” ETSI, December 16, 2022. <https://www.etsi.org/about>.

Multilateral fora

Except for some successes such as the TGA Principles, high-level multilateral declarations on data flows still need to be implemented and discussions at various multilateral fora are currently disconnected. Therefore, there is a need for continued commitment between these fora; going from political agreement, to operation, to binding agreement and practical enforcement. Existing multilateral fora would focus on their most appropriate role, whether that is high-level agreement (e.g. G7, G20), technical operationalisation (e.g. CBPR or approval of technical protections that could be recognised as transfer tools) or oversight of binding agreements (e.g. WTO or regional trade blocs) or other inter-country enforcement cooperation in relation to data protection decisions.

This was the approach taken for the creation of the Financial Stability Board (FSB). The FSB emerged from a political commitment at the G20, giving it political support and credibility. The FSB then produces policy proposals, which are passed onto central standard setting bodies such as the Basel committee, or the International Organisation of Securities Commissions (IOSCO) in the case of securities regulation, who would then draw up more specific rules and regulations. The member countries must then implement this domestically, in accordance with the FSB charter.

This approach could be taken to progress a number of initiatives to support technical operation. For example, G7 commitments that can then be developed into more detailed principles or policy by the OECD, and then into technical requirements through the ISO or the Global CBPR. The UK should therefore encourage targeted and meaningful cooperation between different fora according to their specialism, to streamline international data transfers. For example, the UK could aim to ensure that all G7 political declarations are taken forward in other fora.

The Council was informed of this approach by a presentation from Japan's Ministry for Economy, Trade and Industry, setting out its plans for a new Institutional Arrangement for Partnership (IAP) to operationalise "data free flow with trust"⁶⁷. With the establishment of the IAP proposed during Japan's presidency of the G7, which would advance the concept of "data free flow with trust" and international cooperation and trust on digital governance issues, the IAP will fill a critical gap by bringing together like-minded governments and stakeholders to drive meaningful progress on digital and data governance issues in ways that protect both public safety and individual rights, including privacy, while strengthening consistency of policy frameworks across jurisdictions.

Key characteristics of a successful multilateral approach are not duplicating existing work, promoting close cooperation between governments and private stakeholders, and taking forward concrete projects. The Council examined the question of the desirability of a new global body in the light of the calls for a "New Deal for Data" or a "Financial Stability Board or Bretton Woods of Data", to avoid any unjustified restrictions or hindrances on international data transfers, and to facilitate instead a single data governance model that goes beyond Convention 108+. This is a view expressed by several stakeholders.

The table on the next page presents a summary overview of four plausible future scenarios for the international data ecosystem of 2030, depending on how global availability of data (increased/decreased) and global data governance frameworks (cohesive/fragmented) evolve over the next 8 years. "Data blocs" represent the current dominant trend.



“Key characteristics of a successful multilateral approach are not duplicating existing work, promoting close cooperation between governments and private stakeholders, and taking forward concrete projects”

⁶⁷ <https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-annex-g7-digital-and-tech-track-annex-1-g7-vision-for-operationalising-dfft-and-its-priorities>

Open access freely available data

Fragmented Global Governance	<p>Data Blocs (dominant trend)</p> <ul style="list-style-type: none"> Declining multilateralism Fragmentation of data systems Upsurge in domestic regulatory actions Considerable variation in approaches to national security Global Britain is too small to compete 	<p>Global Data</p> <ul style="list-style-type: none"> A single data governance model Information flows freely across sectors and borders Rising digital inequality. Data is hard to commercialise Previously protectionist countries have lowered restrictions 	Cohesive Global Governance
	<p>Data Islands</p> <ul style="list-style-type: none"> Multilateralism has collapsed. Reduced trade, competition and personal privacy Power and innovation concentrated in the hands of Big Tech Extreme public attitudes on data use An isolated UK 	<p>Data Lords</p> <ul style="list-style-type: none"> One superbody global institution Access to data restricted by big business monopolies Competition between Big Tech is rife High public distrust UK allies have not changed 	

Commercialised data and concentrated market power

Given the plethora of existing multilateral fora, there was concern that introducing a new body into the current landscape risks merely adding another imperfect forum to the already fragmented ecosystem. A new body could be seen as an alternative if the short-term and medium-term recommendations do not result in improvements in sustainable and scalable international data transfers. Only if the recommendations in this report fail to achieve the desired objective should the UK consider suggesting a new global body to facilitate international data transfers.

Regulation and enforcement on a global scale

The Council considered the role of enforcement of agreed principles and standards for both industry and states. The point was raised that enforcement is not necessarily the best way of achieving compliance, especially in areas with complex rules (like financial regulation - but also data protection), where research has shown that improved overall compliance is best achieved by guiding actors towards compliance, rather than constant enforcement.⁶⁸ In that

⁶⁸ See CIPL Discussion Paper on “Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability”, 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

context, Professor Hodges' work on regulation and enforcement was raised⁶⁹ and he was invited to present his research. Much research indicates that, in the absence of a global government or equivalent (e.g., a centralised international data governance institution), a prescriptive approach to compliance relying solely on sanctions is not viable, as sanctions still take place at the nation-state level. Furthermore, evidence suggests that deterrence and punishment does not function as an effective compliance model.⁷⁰

Instead, an "Outcome-Based Cooperative Model" for compliance is proposed, which would put the onus on organisations to be accountable for operating in accordance with the external rules and internal policies, and on constructive engagement and cooperation between interested and affected parties, including regulators and regulated entities. This should not replace all need for sanctions and appropriate oversight but should be based on trust between organisations and trust in the respective countries' data protection regimes. Much like in the aviation sector, successful regulation should be based on a performance model, accepting that flaws will be identified, and some mistakes are inevitable, but with a continuous drive for an improvement in performance, there will be continuously higher standards.

This approach would also incorporate and incentivise organisational accountability and will expect that the organisations implement policies, controls, procedures, and technologies to comply with data protection requirements in respect of international data transfers and ensure accountability and protection flows with data. The UK should consider and promote globally how regulators and policy makers incentivise good organisational practices and accountability in international data transfers, to deliver long term positive changes in behaviours and legal certainty. Alongside pushing for continuously higher standards, the UK can leverage third-party verifiers as accountability mechanisms, to extend the reach of regulators, and to build trust in countries whose regulators are still maturing.

Many countries have developed comprehensive data protection regimes but have not yet established a regulator, found an effective way to resource the new regulatory body, or are focused on compliance capacity-building with domestic industry, rather than spending limited resources on large-scale enforcement. Engagement with these countries could focus on how to develop these structures, whilst recognising that the countries themselves are best placed to determine how these should be operationalised. The World Bank and the Inter-American Development Bank provide grants and financing to developing countries, and the UK could work through these institutions to suggest financing for the fleshing out of data protection regimes, to allow high-growth countries to take advantage of the economic and innovation possibilities of international data transfers. The Commonwealth or the UN could also take a role in coordinating this work.

It is important to engage with countries who are developing data protection regimes, such as Chile, Thailand, Vietnam, Argentina, and Nigeria. The Council



“The UK should consider and promote globally how regulators and policy makers incentivise good organisational practices and accountability in international data transfers, to deliver long term positive changes in behaviours and legal certainty”

⁶⁹ See C. Hodges, Outcome-Based Cooperation: in Communities, Organisations, Regulation, and Dispute Resolution (Hart, 2022); see C. Hodges and R. Steinholtz, Ethical Business Practice and Regulation: A Behavioural and Values-Based Approach to Compliance and Enforcement (Hart, 2017); see also C. Hodges, Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Culture and Ethics (Hart Publishing, 2015).

⁷⁰ See C. Hodges, “Ethical Business Regulation: Understanding the Evidence”, 8, February 2016, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/497539/16-113-ethical-business-regulation.pdf

was particularly interested in India's upcoming data protection law and viewed India as a key engagement partner on data matters. India's data protection law has the potential to be influential as a model in high-growth countries, and as such could have wide-ranging consequences. The UK should work actively with other countries and engage where appropriate to promote a regime with mutual benefits which is conducive to data flows and enables India to play an important role in any future multilateral mechanisms of international data transfers.

Key findings

There are some immediate priorities to address to facilitate international data transfers, which require action at different levels and not simply by the UK. **Some of the activities discussed here cannot be achieved through the UK acting alone and the focus must be on engagement with other countries and multilateral fora.**

Work must be done toward **developing and agreeing on common data protection standards for international data transfers to third countries** (setting objectives on the basis of the OECD Privacy Guidelines for example).

The UK should **make better use of, evolve, and simplify alternative transfer mechanisms** such as SCCs and BCRs.

The UK should **promote certification to certain industry standards being accepted as international data transfer tools** under UK GDPR to facilitate international data transfers.

Incentivising good practice is likely to lead to a higher overall level of compliance than regulatory penalties alone.



“Incentivising good practice is likely to lead to a higher overall level of compliance than regulatory penalties alone”

EXPERT COUNCIL BIOGRAPHIES

Vivienne Artz OBE FCSI (Hon)

International Regulatory Strategy Group; Global Legal Entity Identifier Foundation Non-Executive Director and PICCASO Vice Chair

Vivienne is a board director and advisor, strategic consultant and expert on data and privacy, financial crime and inclusion & diversity issues, with over twenty years' experience in the financial services sector. Her current roles include Data Strategy and Privacy Policy Advisor to CIPL, Director to Global Legal Entity Identifier Foundation and Freegold Ventures Ltd, Board Advisor to Privacy Culture, Vice Chair of PICCASO and founder of the PICCASO Privacy Awards, Expert Advisor to GSS-Rose Limited, Chair of the Global Coalition to Fight Financial Crime Privacy Committee and Honorary Fellow of the Chartered Institute of Securities & Investment. Vivienne also advises a range of innovative, fast growth technology companies, is an expert advisor to New Financial, and Chapter co-lead of the City of London Finance for Growth initiative.

João Barreiro

BeiGene, Chief Privacy Officer, Executive Director

João is a privacy executive with a long experience in designing and implementing privacy programs in multinationals operating in the pharmaceutical, IT and financial sectors. Based in London, he is the Chief Privacy Officer of BeiGene, a global biopharmaceutical company. João also serves as a board member of different associations, including the Research Advisory Board of the International Association of Privacy Professionals (IAPP), the International Pharmaceutical and Medical Device Privacy Consortium, and the Digital Trade Policy Taskforce of the Biotechnology Innovation Organization. He is also co-author of the book 'Privacy Program Management'. In 2022, João was recognized as Privacy Executive of the Year by the PICCASO Privacy Awards, and in 2020, he was listed as a 'Global Top 100 Data Visionaries'.

Bojana Bellamy

CIPL, President

Bojana is the President of Hunton Andrews Kurth's Centre for Information Policy Leadership (CIPL), a preeminent global privacy and data policy think tank in London, Washington, DC, and Brussels. Bojana works with global business and technology leaders, regulators, policy and law makers to shape global data policy and practice and develop thought leadership and best practices for privacy and responsible data use. In 2019 Bojana received the IAPP Vanguard Award, which recognizes privacy professionals for outstanding leadership, knowledge, and creativity. With over 25 years of experience in privacy and data policy and compliance, including former global privacy head at Accenture for 12 years, she sits on several industry and regulatory advisory boards and panels.

Ruth Boardman

Bird & Bird, Co-head of International Privacy and Data Protection

Ruth is co-head of Bird & Bird's International Privacy and Data Protection Group. Ruth has extensive experience advising a broad range of organisations on data privacy matters. Ruth advises on the data protection aspects of new products or services, on commercial arrangements involving personal data, and where there has been a personal data breach. Ruth advises clients on their dealings with data protection authorities and with those involved in passing new data protection legislation. Ruth has written or edited a number of the leading texts and journals on data protection. She is currently a Board Member of the International Association of Privacy Professionals.

Thomas Boué

BSA | The Software Alliance,
Director General of Policy (EMEA)

Thomas Boué oversees the BSA | The Software Alliance's public policy activities in Europe, the Middle East, and Africa. He advises BSA members on public policy and legal developments and advocates the views of the enterprise software sector with both European and national policymakers. He leads on security, privacy and international data flow issues, as well as broader efforts to improve intellectual property protection and promote open markets, fair competition, digital trade and technology innovation in areas such as AI and cloud computing. He led BSA's work as an Amicus Curiae on the Schrems II case on Standard Contractual Clauses at the CJEU and the La Quadrature du Net case on the Privacy Shield at the EU General Court.

Chris Calabrese

Microsoft, Senior Director of Global Privacy Policy

Chris Calabrese is the Senior Director of Global Privacy Policy at Microsoft where he helps lead the company's global public policy work on privacy issues. He previously worked in senior roles advocating for the responsible use of new technologies at the Center for Democracy & Technology and the American Civil Liberties Union (ACLU). Chris has also led several national ACLU campaigns on privacy and was named one of Washington's Top Lobbyists by *The Hill* newspaper. Chris is a graduate of Harvard University and holds a J.D. from the Georgetown University Law Center.

Kate Charlet

Google, Director for Data Governance

Kate Charlet leads Google's Privacy, Safety, and Security Center of Excellence within the Government Affairs and Public Policy team. Her global team of subject matter experts address matters relating to privacy, security, children's policy, and government access to data, and she co-leads Google's public policy response to the war in Ukraine. Kate has spent most of her career at the intersection of technology and public policy. She was previously the inaugural director for Technology & International Affairs at the Carnegie Endowment for International Peace and spent a decade as a civil servant in the U.S. government, including as the Deputy Assistant Secretary of Defense (acting) for cyber policy, country director for Afghanistan, and director for strategic planning at the White House National Security Council.

Theodore Christakis

University Grenoble Alpes,
Professor of International and European Law

Theodore Christakis is Professor of International and European Law at University Grenoble Alpes (France), Director of Research for Europe with the Cross-Border Data Forum, Senior Fellow with the Future of Privacy Forum and a former Distinguished Visiting Fellow at the New York University Cybersecurity Centre. He is also Chair on the Legal and Regulatory Implications of Artificial Intelligence with the Multidisciplinary Institute on AI (ai-regulation.com). He has been a member of the French National Digital Council, and he is currently serving as a member of the French National Committee on Digital Ethics. He recently served as an external consultant for the OECD negotiations which led to the adoption of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.

Fergus Allan Cloughley

International Data Flows Ltd, CEO and Director

Fergus Cloughley, Chief Executive Officer of International Data Flows Ltd, and co-author of The OBASHI Methodology and co-architect of the Obashi technologies. Fergus has spent 25 years researching and developing the fundamental principles, rules and laws that govern the mapping and modelling of cross border data flows. Fergus has been working with the World Economic Forum and associated governments as an advisor and is co-author on various data flow related papers. He is currently involved on national and international dataflow initiatives and projects, for governments, standards and national infrastructure bodies.

Professor Elizabeth Coombs

University of Malta, Associate Professor;
Australian Privacy Foundation, Chair of the
International Committee

Elizabeth was independent consultant to the inaugural UN Special Rapporteur on the Right to Privacy from 2016 to 2021 and chaired the UN Special Rapporteur's Taskforce on 'Privacy and Personality' preparing reports on 'Privacy and Children', and 'Privacy: A Gender Perspective' presented to the UN Human Rights Council in 2021 and 2020. Elizabeth is Chair of the International Privacy Committee of the Australian Privacy Foundation, and recent work includes book chapters on 'human rights and technology assisted violence'; 'Governance for AI - let's not forget gender', and her next book chapter concerns human rights for children and AI in educational technologies.

Nigel Cory

ITIF, Associate Director for Trade Policy

Nigel Cory is an associate director covering trade policy at the Information Technology and Innovation Foundation. He focuses on cross-border data flows, data governance, intellectual property, and how they each relate to digital trade and the broader digital economy. He has provided in-person testimony and written submissions and has published reports and op-eds relating to these issues in the United States, the European Union, Australia, China, India, and New Zealand, among other countries and regions, and he has completed research projects for international bodies such as the Asia Pacific Economic Cooperation and the World Trade Organization. He previously worked for eight years in Australia's Department of Foreign Affairs and Trade.

Caitlin Fennessy

IAPP, Vice President and Chief Knowledge Officer

Caitlin Fennessy is Vice President and Chief Knowledge Officer at the International Association of Privacy Professionals. In this role, she guides the strategic development of IAPP research, publications, communications, programming and external affairs. Caitlin served previously as the Privacy Shield Director at the U.S. International Trade Administration, spending ten years working on international privacy and cross-border data flow policy issues. Caitlin was also an adjunct professor of international privacy law at the University of Maine School of Law and University of New Hampshire School of Law.

Kuan Hon

Dentons, Of Counsel, Privacy and Cybersecurity

Dr W Kuan Hon is an English solicitor and New York attorney, with degrees in both law and computing science. Her practice focuses on UK/EU data protection, privacy, e-privacy and cybersecurity laws, but with broader data/digital/tech regulatory expertise especially in cloud computing, digital services/online platforms and artificial intelligence/machine-learning. She advises organisations, particularly international groups with cross-border operations, on all aspects from strategy and compliance to operationalisation, ongoing governance, and incidents/investigations. She was also a guest lecturer for Imperial College London's Department of Computing. Kuan is the author of Data localization laws and policy - the EU data protection international transfers restriction through a cloud computing lens (Edward Elgar) and lead author of several chapters of Cloud Computing Law (OUP) as well as many other publications.

Caroline Louveaux

Mastercard, EVP/Chief Privacy Officer

Caroline Louveaux is the EVP/Chief Privacy Officer for Mastercard. She leads the company's work at the forefront of the policy, regulatory and legal compliance on privacy and data protection globally. Caroline spearheaded Mastercard's global adoption of the EU General Data Protection Regulation as well as the adoption of Mastercard's Binding Corporate Rules and APEC Cross-Border Privacy Rules to safeguard the future of Mastercard's global data flows. Caroline serves on the Executive Board of the IAPP and is a member of the UK FCA Synthetic Data Expert Group.

Professor Neena Modi

Imperial College London, Professor of Neonatal Medicine; Chelsea and Westminster NHS Foundation Trust, Consultant

Neena is Professor of Neonatal Medicine at Imperial College London, one of the world's top ten universities, Consultant at Chelsea and Westminster NHS Foundation Trust, an elected fellow and member of council of the prestigious UK Academy of Medical Sciences, and a past-president of the British Medical Association and Royal College of Paediatrics and Child Health. She leads a multidisciplinary research group focused on improving the care and life-long health of preterm and sick newborn babies. She established the award-winning UK National Neonatal Research Database, and most recently, a new International Neonatal Research Database.

Peter Swire

J. Z. Liang Chair, Georgia Tech School of Cybersecurity and Privacy

Peter also works as Professor in the Scheller College of Business, is Senior Counsel with Alston & Bird LLP, and is Research Director of the Cross-Border Data Forum. In 2019, the Future of Privacy Forum honoured him for Outstanding Academic Scholarship. In 2018, he was named an Andrew Carnegie Fellow for his project on cross-border data flows. In 2015 the IAPP awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Under President Clinton, he was the Chief Counselor for Privacy, the first person to have U.S. government-wide responsibility for privacy policy.

Huey Tan

Apple, Head of Privacy Policy and Regulation APAC

Huey's legal experience includes privacy and data protection, intellectual property rights, information technology, and legal and regulatory affairs. He is the first President of AsiaDPO, a Singapore registered society of Data Protection Officers (DPO) and served as a non-government expert to Singapore's Public Sector Data Security Review Committee (PSDSRC) in 2019. Prior to Apple, he held senior roles in data governance and legal policy at Accenture, Skype, and Microsoft. He started as an IP litigation lawyer at Baker McKenzie Hong Kong working on software copyright issues for a variety of IP owners, including games and software. He has a Master's degree in Digital Media from Swansea University and taught Cyber Law at the LSE's Department of Law.

Eduardo Ustaran

Hogan Lovells, Global Co-head of Privacy and Cybersecurity

Global co-head of the Hogan Lovells Privacy and Cybersecurity practice Eduardo Ustaran is widely recognized as one of the world's leading privacy and data protection lawyers and thought leaders. With over 25 years of experience, Eduardo advises multinationals and governments around the world on the adoption of privacy and cybersecurity strategies and policies. Eduardo has been involved in the development of the EU data protection framework and was listed by Politico as the most prepared individual in its 'GDPR power matrix'.

Richard Ward

IBM, Government Relations Director

Richard Ward is a member of IBM's government and regulatory affairs team for the United Kingdom. Based in London, he has responsibility for policy issues affecting IBM and broader UK business. He is Chair of the techUK working group on data protection and a member of other business data protection groups. He has spent the majority of his career in IBM in a variety of technical, sales and management roles as well as a period in government as an advisor on regulatory policy. Richard has a particular interest in data protection and the ethical deployment of AI, cyber security and on the impact of technology adoption on competitiveness.

Dr Isaac Rutenberg

Director of the Center for Intellectual Property and Information Technology Law

Dr. Isaac Rutenberg is an Associate Professor of ICT Policy and Innovation at Strathmore University in Nairobi, Kenya. He is the founder of the Centre for Intellectual Property and Information Technology Law (CIPIT), also at Strathmore University, and served as the Director of CIPIT from 2012-2022. His academic research includes a focus on international issues pertaining to data protection, data governance, and artificial intelligence, particularly as they relate to the Global South. Prior to joining academia, he worked as a patent lawyer in California. He holds a PhD from Caltech and a J.D. from Santa Clara University.



OGI

© Crown copyright 2023

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at:
alt.formats@beis.gov.uk