TheCityUK

Digital trade: a commercially viable approach

What the UK-based financial and related professional services industry needs for digital trade and why

About TheCityUK

TheCityUK is the industry-led body representing UK-based financial and related professional services. We champion and support the success of the ecosystem, and thereby our members, promoting policies in the UK, across Europe and internationally that drive competitiveness, support job creation and ensure long-term economic growth. The industry contributes 12% of the UK's total economic output and employs over 2.2 million people, with two thirds of these jobs outside London. It is one of the largest exporters and generates a trade surplus exceeding that of all other net exporting industries combined. It is also the largest taxpayer, and makes a real difference to people in their daily lives, helping them save for the future, buy a home, invest in a business and protect and manage risk.

Contents

Foreword

Global data governance is one of the most important global challenges of our time.

Globalisation and digitalisation have transformed the world economy by enabling the creation of integrated businesses that are powered by international digital supply chains. Digital supply chains allow businesses to leverage the diverse talents of the best and brightest employees in a huge range of geographic markets to provide an unparalleled service to their global clients and customers.

International data flows power digital supply chains: businesses need them to create new products and services, interact with customers and clients, enable cross-border working, and provide mission critical functions like cybersecurity and data protection.

The financial and related professional services industry has adapted well to digitalisation and shaped global operations that leverage a globally diversified set of digital and technology functions. Financial and related professional services businesses source data from all of the markets they operate in, and store, access and process data internationally in order to provide a secure and efficient service to consumers and business end users on a 24/7 basis.

However, well established global business models are increasingly challenged by a surge in digital protectionism. Restrictions on international data transfers have more than doubled since 2017. Digital protectionism is raising the cost of doing business and restricting consumer choice and competition, preventing individuals and businesses from accessing the world's best technology solutions.

Digital protectionism is a major and growing threat to global commerce. While many digital trade restrictions have been implemented with good intentions, data localisation measures and other limitations on data flows strike at the heart of global supply chains.

This paper aims to inform policy discussions about digital trade by explaining why digital trade is pivotal to the proper functioning of businesses and outlining the commercial and operational challenges that businesses face with digital trade. It will make recommendations about how the UK and international governments can resolve these challenges and deliver on the digital policy objective agreed by the G20: "data free flows with trust".[1]

Digital protectionism has wider consequences than economic disruption. Because data is invisible, restrictions on its movement are often overlooked in comparison to restrictions on the movement on goods. But in a highly digitalised world, digital supply chains are just as important as physical supply chains. Policymakers should treat their fragmentation just as seriously.

1 The policy recommendations in the paper draw freely on a range of findings from across the UK-based financial and related professional services industry, including Making the UK the leading global financial centre: An international strategy for the UK-based financial and related professional services industry (TheCityUK, 2021), Past precedent and future opportunities: assessing digital trade provisions for the UK FPS sector (The City of London Corporation, June 2021), and The future of international data transfers (International Regulatory Strategy Group, April 2022).

Left unchecked, digital protectionism looks set to become the 21st century equivalent of the tariffs imposed by countries in the 1930s: measures that sparked economic decline and heightened geopolitical conflict. It must also be remembered that individuals rely on data flows as much as businesses and governments: in developed and developing countries alike, individuals increasingly discover the world through digital channels, forming political, social, and cultural views based upon the information they encounter online. If digital protectionism continues to rise, people in all markets will suffer from restricted access to information, and need to rely on limited domestic information sources to form their view of the world. A world in which digital protectionism creates a 'splinternet' will be a world in which people in different countries lose the ability to learn from each other and interact with each other – a world in which people will be poorer in every sense of the word.

For economic, political and cultural reasons, it is vital that data can continue to flow freely across borders, and that governments work together to make this possible. While there is much that countries can do by themselves to strengthen their own data policies, and this report suggests ways in which the UK can do this, ultimately the governance of cross-border data flows is a global public good issue and needs to be addressed as such, with a new global agreement backed by a new global institution. This paper suggests ways in which a global agreement on data flows might be initiated. The UK-based financial and related professional services industry is ready and willing to work with governments and regulators around the world to make this vision a reality.

Miles Celic

Chief Executive Officer, TheCityUK

Executive summary

This report provides a commercial perspective on how the UK-based financial and related professional services industry views digital trade and what industry needs in terms of digital trade in order to support its global clients and customers in a safe and efficient way.

Digital trade is the exchange of assets, goods and services that are delivered electronically, within or between companies or a company.

Financial and related professional services businesses have been highly digitalised for a long time, meaning that trade in financial and related professional services is overwhelmingly digital trade: 86% of UK financial exports are digitally delivered.

Over the last 30 years, financial and professional services businesses have developed global operations that are optimised to benefit from global data flows. Businesses need data flows to conduct due diligence on supply chains, make investments, draw on the abilities of a global talent pool to support customers and clients, fight financial crime, and provide cybersecurity functions.

What are the main operational challenges to digital trade?

To perform these essential functions, businesses need to source data, store data in safe locations, access data to perform core business functions, and process data in appropriate locations. However, recent policy changes in many countries are threatening these established business models, raising costs, and restricting choice for businesses and consumers.

Digital trade barriers doubled between 2009-2019, and restrictions on international data transfers have more than doubled since 2017. This is a problem because businesses rely on digital trade to support their customers and clients. The main policy challenges facing industry businesses include:

- Data localisation measures which make it hard for businesses to support their clients, push companies to leave some markets and avoid entering others, threaten data protection, and undermine the fight against financial crime.
- Regulatory requirements that make it hard for UK businesses to work with global partners, restrict growth opportunities, and limit consumer choice.
- An onrush of divergent regulations which businesses need to reconcile to view basic information, and which push up costs for clients and business end users.
- Uncertainty about how to implement regulations that distinguish sharply between personal and non-personal data when in practice data often fluctuates between the two states.

What solutions should the UK adopt to strengthen its position as a global centre for data and to boost global digital trade?

The UK benefits from a major comparative and competitive advantage in financial and related professional services and, provided data can flow freely across borders, could become a global centre for storing, accessing and processing financial and related professional services data. The UK would then benefit from greater innovation, a wider choice of digital services, and more high skilled jobs and sustainable development.

To achieve this goal, the UK government and regulators should facilitate digital trade by refining UK data policies and agreeing new bilateral and multilateral digital partnerships.

The UK's ultimate goal should be to secure a global agreement on data that realises the G20 ambition of "data free flows with trust". In the meantime, the UK should optimise international data flows where it can, removing digital frictions wherever possible and avoiding raising new digital trade barriers. The recommendations below set out the key steps the UK should take.

Key recommendations

Policy changes that the UK government and regulators should make unilaterally

- UK data regulators should provide more practical examples to businesses to explain how to handle data that is not clearly "personal" or "non-personal" from a regulatory perspective. Industry is eager to work with government and data regulators to shape Codes of Conduct that provide this guidance.
- UK data regulators should provide more practical examples and use cases to financial institutions that set out the circumstances in which they may share their customers' personal data with other financial institutions in order to make them aware of potential financial crimes.
- UK data regulators should create an information bank that provides data on the risk profiles of various international data regimes. This information bank should be a shared resource that could be accessed by businesses when making Transfer Risk Assessments.
- The UK government should avoid domestic localisation measures where possible including, for example, when implementing the Telecommunications (Security) Act 2021 and offering government procurement.
- The UK government should review the UK's subsea data cables every two years to ensure that they are fit for purpose. Government should publish findings on the resilience of the UK's digital infrastructure and recommendations to strengthen it.

Policy changes that the UK can agree bilaterally with international partners

- The UK government should agree Free Trade Agreements (FTAs) that prevent unjustified data localisation laws, protect digital intellectual property, prevent customs duties on electronic transmissions and support a risk management based approach to cybersecurity. The digital provisions in the UK's FTAs with Japan and Australia, and the UK-Singapore Digital Economy Agreement provide models to replicate elsewhere.
- The UK government should use bilateral economic dialogues (e.g. Economic & Financial Dialogues) to urge countries imposing data localisation laws to avoid restrictions on the movement of offshore data and allow their citizens' data to flow to at least some markets, even if not all markets.
- The UK should use financial regulatory dialogues to urge countries that have imposed data localisation requirements to grant financial institutions targeted exemptions from localisation requirements to perform anti-money laundering and cybersecurity checks.
- UK data regulators should consider whether to extend data adequacy assessments to countries like Australia, Singapore and South Korea provided they are satisfied that their data standards are comparable to UK standards.
- The UK should use bilateral regulatory dialogues and regulation chapters in FTAs to bind other countries to follow good digital regulatory practices. Countries should announce proposals to impose data localisation in good time and justify why – this will give businesses a chance to propose alternatives.
- The UK should use bilateral financial regulatory dialogues to ensure that the regulators of the UK's main trade partners can provide a secure portal through which businesses can share encrypted information.
- UK regulators and the regulators of other key financial centres should conclude financial data connectivity agreements that set out the importance of enabling free data flows with trust for financial data and avoiding localisation of financial data. The US-Singapore Joint Statement on Financial Services Data Connectivity provides a good model to follow.

Policy changes that the UK needs to realise through global co-operation

- The UK should work with members of the World Trade Organization (WTO) Joint Statement Initiative on E-Commerce to conclude a WTO E-Commerce Agreement that prevents unjustified localisation measures (including on financial data), protects digital intellectual property, prevents customs duties on electronic transmissions, and supports a risk management based approach to cybersecurity.
- The UK should work with the Global Cross Border Privacy Forum, EU, and other partners to shape a global data agreement whereby regulators agree to common standards for recognising the validity of each other's personal and non-personal data regimes. Regulators could consider if Council of Europe Convention 108 on Data Transfers or OECD Guidelines on Transborder Flows of Personal Data provide a sufficient basis for data protection, especially if tailored to cover all data flows, not only personal data.

What is digital trade?

Digital trade is a commonly used but contested term. From a policy perspective, digital trade is widely taken to encompass three distinct policy areas:

- The rules that decide the terms under which data can be stored, transferred, accessed, processed, and sold.
- The rules that cover the digitalisation of trade – for example, outlining whether customs checks or trade finance documentation can be digitalised.
- The rules that regulate digital markets - an increasing share of global value chains is being captured by digital activity.[2] Policymakers are moving to regulate emerging digital markets by framing new laws that boost competition in data provision, regulate healthtech, or ensure cybersecurity. Many new such regulations could potentially constitute trade barriers.

However, from a business perspective, digital trade is best defined as the exchange of assets, goods and services delivered electronically, within or between companies or a company.

Different industries are affected by digital trade in different ways. The fact that customs checks often require customs officials to read lots of paper forms affects businesses moving goods across borders and trade finance providers more than most services businesses, for example.

Financial and related professional services businesses are distinctive in that their products and services are already almost wholly digitalised and have been so for a long time. 86% of the UK's global financial services exports, and 90% of its insurance exports, were digitally delivered in 2019.[3] The biggest digital trade barriers affecting the industry are therefore those that make it harder to store, transfer, access and process data across borders.

This paper will identify the key frictions financial and related professional services businesses face and explore how policymakers can ease such frictions.

2 Many previously non-digital products are becoming digitalised, such as newspapers and cloud-based HR and expense management services. Other non-digital products are having their value transformed by digitalisation: steel businesses, for example, often extract as much value from data about steel as from steel.

3 Digital Trade: A Board of Trade Report (Board of Trave, November 2021), Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035370/digital-trade-a-board-of-trade-report.pdf

How does digital trade work within a business?

Digital trade is essential for running a global financial or related professional services business. As information and communications technologies transformed the world of work over the last thirty years, financial institutions adapted to create efficient global businesses that relied on the ability for data to flow across borders with relative ease.

Digitised data is core to almost all of the products and offerings that financial and related professional services offer to their customers and clients. Beyond this, businesses rely on data flows to perform essential back office and middle office functions.

The examples set out below provide further context about some of the main ways in which financial and related professional services businesses need to use data flows to support clients, make operations more efficient, and seize growth opportunities.

Some examples of why financial and related professional services businesses need digital trade

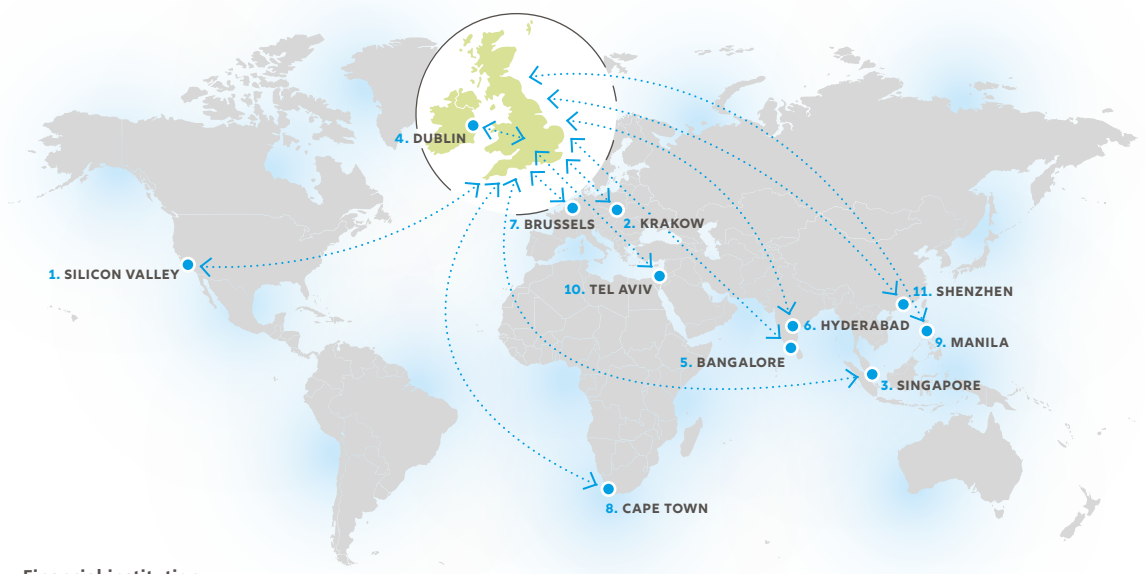
- **Trading and investing:** Financial services businesses need to monitor international data to verify supply chain data, make decisions on trade finance, and evaluate the risk levels of businesses seeking new investment or insurance. Digital trade enables critical due diligence that protects savers and investors.
- **Understanding clients:** Financial institutions often support their clients in many ways. A client might seek support from different subsidiaries of a bank, or from a bank's investment bank and its private bank. To support the client properly, employees need to pool knowledge of the client from across the global business. This is a key part of the value-add that an integrated financial institution offers – to provide better advice after gaining a holistic understanding of their clients' strategies over time.
- **Providing expert advice:** Financial and related professional services often draw on expert international talent when advising clients. But this means that teams in one country need to be able to source expertise from another market, whether via emails, Teams or case studies.
- **Offering clients a 24/7 service:** Many firms offer a "follow the sun" service so that they can help clients 24/7. To do this, teams need to task international colleagues to work on a project after their own working day finishes. For example, a team in India might conduct research work for UK colleagues so the work can be shared with the client the next day.

- **Delivering an efficient support service to customers:** A global business can service customers and clients more efficiently from some jurisdictions than others. North Africa is a sensible place from which to provide French speaking clients with a French speaking technology service. India makes more sense for an English client base. Singapore is a sensible place from which to offer blockchain services because of the quality of its cryptocurrency regulation. Other locations might provide cost advantages. Businesses need to leverage these geographies of digital trade to be able to efficiently support clients.
- **Providing clients with the best technology solutions:** Businesses want to use the best IT solutions to help them service customers and clients. For example, the Tokyo offices of a UK-based business might want to access a cloud-based provider that stores data in the EU because it provides the best quality service. To get the best service, businesses need to be able to look beyond business partners in their own market.
- **Offering clients strong data protection:** Businesses are moving away from storing data in their own data centres towards using the services of cloud-based providers like Google, Amazon Web Services, Salesforce and Microsoft. Cloud providers offer advantages in efficiency and security. But they are not present in every market – businesses may need to transfer data across borders to store it in the cloud.
- **Regulatory reporting:** Financial institutions need to provide regulators with information about market activity and demonstrate "lineage" on the data they provide. Financial institutions need to show regulators who had access to, and the ability to interact with, the data they provide at different points in its data lifecycle. Data regulations can make it hard for institutions to develop a fully accurate picture of data lineage because they are not allowed to access or share information about who interacted with the data at different points in its lifecycle. This impacts the quality of the information they can provide regulators.
- **Deploying highly-skilled technology talent:** Financial and related professional services businesses hire many software engineers in the UK. However, the UK faces digital skills shortages. To offer the best technology solutions to customers and clients, UK businesses need to employ and communicate with international technology talent.
- **Developing AI:** businesses need access to large data sets and highly specialised technology talent to build successful AI applications. Financial and professional services AI applications are no exception. UK businesses do not have access to such an array of domestic data as US and Chinese based businesses. It is especially important that they can access and process global data when developing AI tools.
- **Preventing financial crime:** Financial institutions need to hold data that monitors financial crime in one place. Financial crime takes place across national borders: it is hard to catch criminals if you can only see what they are doing in one country. Firms need a consolidated global view of client activities to monitor anti-money laundering, and detect and investigate cross-border transactions for money laundering and terrorism financing activity.
- **Protecting clients from cyberrisks:** As cyber threats transcend national boundaries, firms need to be able to share threat intelligence and use several cybersecurity operations centres to safeguard their networks, operation and data. These cybersecurity operations need to be spread across multiple locations to build resilience and avoid having single points of failure. Businesses need to be able to access reserve technology capacity in international markets.
- **Global Enterprise Security:** Modern security architectures depend upon cross-border information sharing and 24/7 follow-the-sun approaches to monitoring network security. Common global security approaches are needed to effectively secure digital trade.
- **Enabling auditing:** Auditing teams need to capture and analyse data from across their clients' business and bring all the relevant data together in the market where the client is listed. The UK is a major centre for international listings and UK-based auditors need to be able to readily access international data in the UK.

While these use cases are presented here as distinct issues, in practice global financial and related professional services businesses need to manage situations relevant to all of these examples every day in a range of different markets. Data management is a complex function that cuts across all areas of a global financial institution, and the digital supply chains that businesses rely on are every bit as complex and globally diversified as physical supply chains.

The infographic below shows the digital supply chain of a global financial institution, outlining the primary flows of data to and from the business.

Figure 1: The digital supply chain of a global financial institution



Financial institution...

1. relies on data flows to investigate FinTech/RegTech investment opportunity in **Silicon Valley**
2. locates data analytics function in **Krakow** to take advantage of highly skilled, multilingual technology talent
3. gathers data from a FinTech operating in **Singapore's** regulatory sandbox to support the development its new digital ID applications
4. stores and processes data stemming from their subsidiary based in **Dublin's** International Financial Centre
5. relies on data flows to access the services of highly skilled software engineers in **Bangalore**
6. outsources work to a skilled, English speaking operations team in **Hyderabad**
7. stores and processes client data and hosts software-as-a-service applications on a cloud-based server in **Brussels**
8. uses a contact centre in **Cape Town** so that customers can benefit from skilled English language telephony
9. uses a contact centre in **Manila** so that customers can benefit from skilled English language telephony
10. accesses leading cybersecurity offerings from **Tel Aviv**
11. operates a joint venture with Chinese payments platforms based in **Shenzen** so that it can enable the payments platforms to be used in the UK

To successfully operate these digital supply chains, create new products and deliver them safely to consumers and business end users, businesses need to **source** data in the markets they operate in, **store** it safely, **access** it for core business functions and **process** it in commercially relevant locations. The key operational requirements for each function are set out in the table below.

Understanding the mechanics of cross-border data flows

Data sourcing

UK-based financial and related professional services business operate in several countries. A law firm might operate in 20+ jurisdictions, and a global financial institution might operate in 50+ jurisdictions. Businesses need to source data from all markets they are active in to support customers and clients.

Data storage

Until recently, global financial institutions tended to store data in their own data centres; they might operate between five and ten data centres in different geographic regions. For security and efficiency reasons, financial and related professional services businesses are increasingly storing data in servers provided by cloud businesses like Google, Microsoft, Amazon Web Services and Salesforce. Inevitably, not all cloud providers have servers in every jurisdiction; and sometimes no cloud providers have servers in a jurisdiction. Businesses need to be able to move data out of jurisdictions to store them with cloud providers.

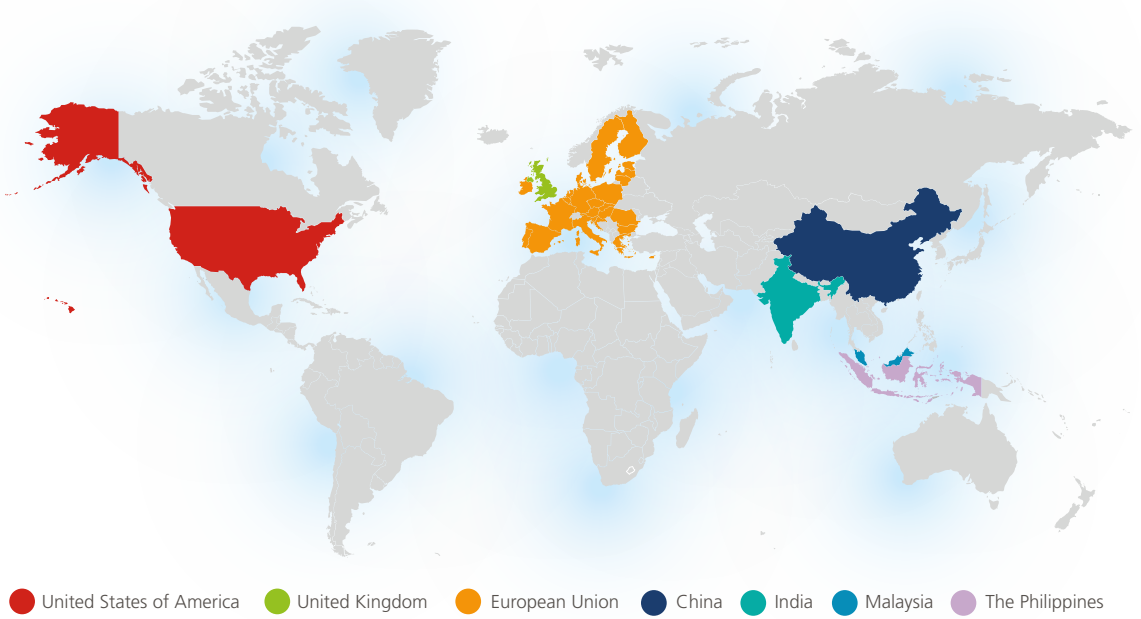
Data access

Businesses need to locate specialised data functions in places which offer high-quality technology talent and infrastructure at a reasonable price. Access to regulatory systems that support high-quality processing is needed so that client data is handled safely and sensibly.

Data processing

Global businesses cannot process data in every market they operate in. Operating in this way might require financial institutions to establish over fifty data processing centres. Anything close to this would be prohibitively expensive, unwieldy, and force a major retreat from global trade. Global businesses need to develop reasonable economies of scale when establishing data processing models. For example, a global financial institution might run one data processing centre in each global region – one in the US, UK, EU, China, India and ASEAN respectively. Key markets in which UK-based financial and related professional services firms locate data processing centres include the US, EU, (especially countries like Poland, Romania and Bulgaria), China, India, Malaysia, and the Philippines, as shown in Figure VII below. Data processing centres are typically located to help businesses support clients on a "follow the sun" model.

Figure 2: Priority locations for financial and related professional services data processing



To manage complex global digital supply chains, businesses need to be able transfer data internationally, process it, and export it back to other markets in which the firm operates.

In the past, businesses were able to do this with relative ease and locate digital operations in the most commercially sensible locations. But increasingly businesses are being forced to neglect commercial considerations when deciding where to locate data functions. An onrush of digital trade barriers in many markets is putting huge pressure on global digital supply chains, forcing firms to either store and process data in a particular market or leave that market altogether.

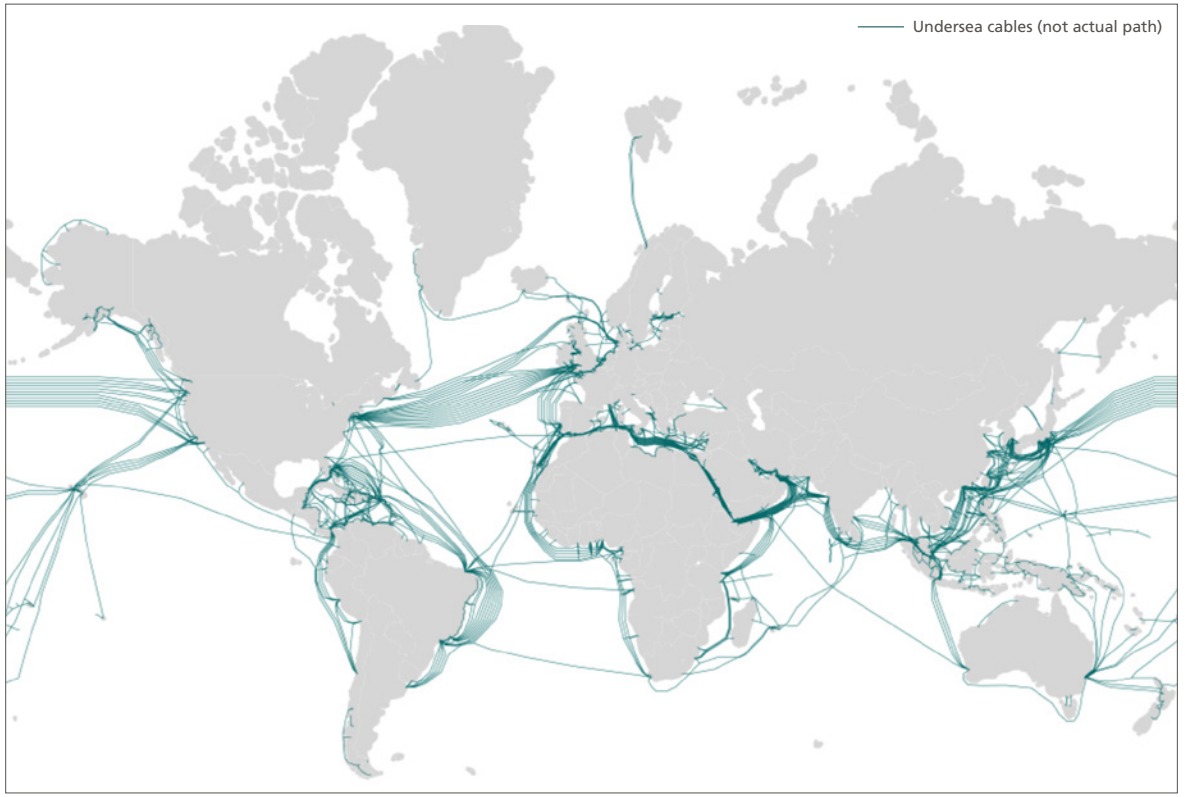
When businesses make decisions about where to transfer, store and process data, they rely on the digital infrastructure that connects their clients and customers to their data storage and processing centres. Submarine cables are by far the most common means of transferring data from one country to another, although satellites look set to replace them over time.[4]

4 US needs to temper reliance on at-risk undersea internet cables, satellites can help (Breaking Defense, February 2022), Available at: https://breakingdefense.com/2022/02/us-needs-to-temper-reliance-on-at-risk-undersea-internet-cables-satellites-can-help-aerospace/

The UK is well positioned as a transatlantic data hub: it is the key node within transatlantic digital trade networks, the point at which US data arrives in Europe via subsea cables and European data flows to the US. (See Figure 3). However, the UK is much less well positioned as a centre for digital trade with rising Asian markets: here, the UK relies on three submarine data cables, all of which traverse the Suez Canal, for its links to the growing markets China, India and South East Asia.

Figure 3: Map of submarine cables

Source: Where are the world's undersea cables? - BBC News



What are the main operational challenges to digital trade?

Policy barriers affecting digital trade have soared, doubling in the decade up to 2019.[5] This report cannot set out all these trade barriers but it will explore two key issues:

- The regulatory and legislative frictions that are making it hardest for financial and related professional services businesses to run a global business in a sensible way
- How to secure digital trade by preventing regulatory divergence on cybersecurity.

Principal regulatory and legislative digital trade frictions

Data localisation measures

Data localisation measures are the most challenging digital trade friction affecting the financial and related professional services industry. Localisation measures require organisations to store or process data in particular jurisdictions. Some highly restrictive measures confine data to jurisdictions. Others permit data to leave jurisdictions provided a data copy is stored on a local server ("data mirroring"). In theory, data mirroring is preferable as it allows cross-border data flows. But data mirroring still forces businesses to duplicate data functions at considerable expense and discourages digital trade.

Data localisation measures have been adopted in many countries in recent years. Governments have often justified localisation measures on the grounds that they are necessary to further entirely legitimate public policy aims like securing their citizens' privacy and personal data, furthering national security and protecting national sovereignty. Businesses support these valid public policy aims and understand the appeal of data localisation measures as a way of delivering on them.

However, in all cases, alternative policies are available which provide more efficient ways of delivering these goals and avoid the damage that localisation causes to global trade and consumer welfare. For example, countries can pass strong protections for their citizens' personal data while still allowing data to flow across borders subject to appropriate governance. Likewise, authorities and regulators can achieve appropriate oversight of data in their jurisdiction for national security purposes without requiring data to be stored in market.

Localisation measures come in many forms. The most common kind of localisation measure requires that the data of citizens of a given country (e.g. China, India, Indonesia) be stored on local servers.

A more severe form of localisation measure restricts the movement of offshored data too. In this case, businesses are prevented from importing data into the market, processing it there, and exporting it again. This second kind of localisation is more trade restrictive. While a business can still locate offshore data processing centres in a country that imposes restrictions only on the transfer of its own citizens' data, businesses cannot locate international data processing centres in countries that impose major restrictions on offshore data. These more all-encompassing localisation measures risk taking entire countries out of global digital networks. India's draft 2019 Personal Data Protection Bill proposed restrictions around offshoring data; Indian policymakers are currently contemplating whether the Bill should be extended to cover non-personal data.[6]

Overall, data localisation can bring "side effects for the financial system and the overall economy: they may increase IT and data complexity; undermine the risk management, cyber security and anti-money laundering practices of financial institutions; as well as reducing access to financial services and markets in some countries."[7]

In addition, localisation measures may have a disproportionate impact on small and medium enterprises (SMEs) due to the exorbitant cost associated with duplicating servers in local market and force businesses, large or small, to choose whether they are willing to stay in market and pay the additional costs or withdraw.

When a country passes data localisation laws, businesses need to decide whether to stay in the market and commit to storing and processing data locally, or whether to withdraw from the market. The table below sets out some of the ways in which businesses think through these decisions.

How do financial and related professional services business respond to data localisation measures?

As businesses conduct their cost/benefit analysis around market presence following data localisation requirements, they often consider the following questions:

- **Does the country's internal market offer sufficient scale to offset the additional costs of business created by localisation requirements?** In recent years, China, India, and Indonesia have passed localisation laws. Many financial and related professional services institutions have decided that the scale of these countries' internal markets justified remaining in the market and establishing local servers. However, businesses report that they have been withdrawing from African markets because of the introduction of data mirroring requirements. Developing markets risk losing their access to global financial institutions by adopting data protectionism. In some countries where there is only one global financial institution present, localisation might cut a country off from international markets and put development at risk. Data localisation measures damage financial inclusion.[8]

5 Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows (June 2020). Available here: http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf, pp7-8 (Accessed 19 May 2021

6 See the latest draft the Indian law (2019). http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. The Joint parliamentary committee which was tasked to review the PDPB still suggested localization in their Dec 2021 report: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

7 Data Flows Across Borders, (Institute of International Finance, March 2019). Available at: https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf

8 The Data Economy: Market Size and Global Trade (Economic Statistics Centre of Excellence, August 2021). Available at: https://www.escoe.ac.uk/publications/the-data-economy-market-size-and-global-trade/

- **Does the country provide exemptions to localisation measures that allow some kinds of financial data to flow freely?** Financial institutions need to be able to transfer data across borders to support core functions such as gathering a global set of financial crime data and tackling cybersecurity. Some countries provide relatively smooth exemptions from general localisation requirements that allow businesses to do this. Other countries make it difficult: this makes it harder for businesses to stay in a market. In Mexico, it is difficult to secure exemptions from localisation requirements and limited cloud provision and this has discouraged UK businesses from entering the market.
- **Do global cloud providers operate in the market?** If global cloud providers operate in the market, it will be easier for businesses to continue to maintain a presence in market despite the localisation laws because they can use the cloud provider's servers when storing data. If cloud providers are not present, businesses will need to establish their own data centres, which is riskier and more expensive and may make a business more likely to leave - or decide not to enter it in the first place. In Saudi Arabia, businesses are required to store data locally despite limited cloud provision. This discourages businesses from entering the market.

Soft localisation measures

Soft localisation measures are legal measures that strongly incentivise businesses to store data locally without formally requiring localisation. Soft localisation measures are sometimes passed by countries who have committed to restrict data localisation in FTAs.

From a business perspective, soft localisation can be as concerning as formal localisation: operationally, it often leads to the same result.

UK-based financial and related professional services firms are currently experiencing soft localisation measures coming from the EU. The EU prioritises competition in the internal market and is therefore restricting EU and UK data transfers to the United States and other international markets, although it has committed in trade agreements to avoid unjustified localisation measures.[9]

After the decision of the European Court of Justice (CJEU) in Schrems II to invalidate the main channel by which UK and EU businesses could transfer data to the US, EU and UK businesses found it increasingly hard to access data solutions from non-EU data suppliers, where the latter were unable to provide a Schrems II-compliant alternative, such as an effective European data boundary. The legal risks of doing so were increasingly evident.[10]

The result is that UK and EU businesses are strongly incentivised to solely rely on technology services offered by data and cloud services providers which operate within EU boundaries and store and process data in the EU. Cloud-based providers reflected this new reality by opting to localise within the EU.[11]

UK and EU Businesses rely on using Standard Contractual Clauses (SCCs) or Binding Contractual Rules (BCRs) to work with non-EU partners. SCCs are used more frequently by businesses than BCRs because the latter are more difficult to establish and operate. The UK has made data transfers easier by shaping a more business-friendly version of SCCs.

Data regulations make it harder for UK businesses to work with clients in the US and Asia

UK data regulations require UK businesses looking to work with international data suppliers to undertake major due diligence efforts before doing business.

International technology suppliers with a limited understanding of UK data regulations often struggle to respond to the lengthy questionnaires that UK businesses need them to fill in - or else provide information that is insufficient or unreliable. Client onboarding becomes much more costly and time consuming than the international partner would reasonably expect, causing tensions in contractual negotiations which can sour business relationships.

UK businesses face a hard choice: either risk non-compliance by working with international partners or rely on EU-based enterprise level data suppliers with templated, pre-packaged due diligence responses. Innovative small and medium sized technology suppliers and international technology businesses now find it increasingly hard to supply services to the UK market.

Market forces are also interacting with regulatory drivers in more subtle ways to nudge businesses towards relying on an ever-smaller pool of familiar partners in familiar markets.

Under UK regulations, businesses need to inform stakeholders via Transfer Impact Assessments of the jurisdictions that their digital service suppliers operate in. Markets like the US, EU/UK and India are widely considered safe. Businesses face questions if data is stored elsewhere, even if the data partner in the alternative jurisdiction is highly reputable. Businesses often find it easier to only work with digital suppliers in familiar markets.

The result of these trends is more consolidation in digital trade and less choice and competition. Fewer countries are included in the global digital economy and the global digital divide is deepened.

Businesses need to assume responsibility for reconciling divergent regulatory rulebooks

Much of the data financial institutions use, such as payments data or anti-money laundering data, can only be understood on an international basis. A payment sent from New York to London cannot be understood by solely by looking at what happened in New York or in London. The full picture can only be seen by looking at both markets. Similarly, a bank cannot track financial crime by consulting data from one jurisdiction; it needs a global view.

9 The UK-EU Trade and Co-operation Agreement digital trade chapter includes commitments to avoid unjustified data localisation.

10 How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime (Information Technology & Innovation Foundation, July 2021). Available at: https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data/

11 Microsoft begins EU data localization process (Global Data Review, May 2021), Available at: https://globaldatareview.com/article/microsoft-begins-eu-data-localisation-process

However, regulation takes place at a national level. This means that different regulations apply to the same piece of data – one set of regulations applies to the payment in New York and another to the same payment in London. To view the transaction, the bank needs to comply with two different sets of regulations.

This is a relatively simple example concerning a single payment. The process is usually far more complicated. A UK business onboarding a client located in China, Singapore and the UAE will need to reconcile UK, China, Singapore, and UAE regulations, define which data is subject to which regulation, and apply that operationally. It will not be able to view its data until it is compliant with all the different standards.

Anti-money laundering efforts require compliance with a vast number of regulations. The burden of deciding which regulations may apply and which rules to follow rests with businesses. And many businesses – especially small and medium sized businesses - may not have immediate access to the resources and legal expertise required to understand potentially applicable laws.

Lack of clarity around how to implement international regulations raises costs and makes it especially hard for small and medium sized business to operate

Businesses reviewing new data regulations often struggle to understand what they mean operationally. Some examples of the vital operational questions businesses often need to struggle with when working out how to apply new rules include:

- Does the new rule require the business to set up a new data centre to be compliant?
- Would it be sufficient to have a hybrid workforce in multiple countries working towards ensuring compliance?
- Does the rule contain a new requirement that only one specific function within the business can analyse data?

The uncertainty around the meaning of new regulations forces businesses to invest considerable resources in contingency planning to assess all the requirements the regulations may have enacted.

Lack of guidance on data regulation forces businesses to hire lawyers and consultants to learn if they can perform basic commercial functions. These additional costs risk being prohibitive for small and medium sized businesses, which might simply opt to leave a market given such barriers.

While a large compliance team can keep track of the new regulations, it is much harder to quantify the scale of the jobs, innovation and value that have been lost because entrepreneurs could not grow a global digital business due to regulatory burdens.

Regulatory uncertainty about the boundaries between personal and non-personal data

UK and EU regulators distinguish between how they treat "personal data" (information relating to an identified or identifiable person) and non-personal data. In response, businesses try to segregate personal data from large data sets and restrict the amount of personal data they collect. Businesses have more flexibility around how they manage non-personal data.

But in everyday life, if not in regulatory texts, personal and non-personal data can be very hard to distinguish. The meaning of data changes based on its context. Some kinds of data (e.g. names) are clearly personal. But in many cases, data only becomes personal when situated alongside other data points that make it possible to use the original data point to identify someone. Data points are often meaningless by themselves and only acquire meaning when mixed with other information sources.

Businesses source data initially in an unstructured form, process it and restructure it. As this process takes place, data will often shift from being personal to non-personal and personal again as the background context changes. Regulations struggle to address the messy realities of data transfer and the regulatory consequences for businesses if they classify data the wrong way are severe.

These ambiguities around whether data is personal or non-personal make it hard for businesses to conduct essential due diligence. For example, insurance businesses need to analyse shipping data to understand the supply chain risks associated with goods being shipped from one market to another. To do this, insurers need to draw together data from bills of lading (often available only in paper form) into coherent digitised data sets. Businesses involved in the supply chain are not always willing to share data about the marine cargo because of fears about breaching personal data protections. They are not sure if the data is personal (in which case it cannot easily be shared) or non-personal (in which case it can). This makes it hard for insurers to evaluate supply chain risks and monitor fraud – a real problem during Covid-19, when it was widely suspected that supply chain fraud rose sharply.[12]

Inevitably, most businesses need to make some guesses when assigning meaning to the limited supply chain data sets that are available and struggle to provide appropriate data governance for each data point at each step of its life cycle. Businesses are exploring technology solutions that help them gain access to relevant supply chain data while not conflicting with regulatory requirements (for example, using blockchain solutions or anonymising personal data). But clear guidance from regulators on how to treat data in practical contexts would be very helpful.

Increasing encroachment of regulators on non-personal data

Until recently, regulators agreed that personal data should be regulated more strictly than non-personal data. The

12 Why COVID-19 made fraud and compliance a bigger issue (EY, April 2021), Available at: https://www.ey.com/en_gl/assurance/why-covid-19-made-fraud-and-compliance-a-bigger-issue

rationale for treating personal data differently was the need to protect individuals' privacy. But increasingly regulators are placing restrictions on commercial and wholesale data. For example, many MENA and APAC jurisdictions are imposing strong outsourcing regulations which trigger additional requirements for regulatory approval when businesses move or process non-personal data outside of their jurisdictions.

Concerns about whether future EU data policy might restrict digital trade for UK businesses

Under UK and EU law, the personal data of UK and EU citizens can only be transferred to other jurisdictions if the relevant authorities consider that their personal data protection standards are "adequate". UK and EU financial and related professional services businesses rely on the UK-EU data adequacy agreements – under which the UK and EU recognised each other's data protection regimes as adequate – to transfer, store and process data in the EU and UK.

Businesses in the UK and EU want to maintain UK-EU adequacy: if it lapses, they will need to establish different sets of data compliance in the UK and EU, raising major barriers to digital trade and increasing the cost of doing business. By contrast, industry businesses rarely rely on UK adequacy agreements with non-EU markets. Industry would therefore not wish to put UK-EU adequacy at risk by concluding adequacy agreements with non-EU markets that do not offer high level of data protection.

Aside from adequacy, the main method that UK businesses rely on to transfer personal data to non-EU markets are SCCs and, to a lesser extent, BCRs. In April 2022, the EU and the US announced an agreement in principle to create a new mechanism to enable personal data transfers between the two markets.[13] It is to be hoped that such a mechanism can be agreed this year. However, businesses remain concerned about whether the CJEU may move in future to invalidate SCCs as a method for transferring personal data outside of the EU should it revisit its previous jurisprudence on data transfers.[14] If the ECJ were to make such a decision, it would be very difficult for UK businesses to share personal data internationally.

How to secure digital trade by preventing regulatory divergence on cybersecurity

Cybersecurity is fundamental to digital trade, just as threats to cybersecurity undermine confidence in digital services and data flows. Financial and related professional services businesses take their responsibilities to protect their customers and clients very seriously, and are eager to see consistent global standards that embed high standards of cyber-protection into global business practices.

Common risk-based approaches to enterprise security supported by international standards, such as ISO/IEC 27110 (which provides guidelines on developing a cybersecurity framework) and ISO/IEC 27103 (which provides guidance on how to leverage existing standards in a cybersecurity framework), the NIST Cybersecurity Framework, or the Financial Sector Profile, help businesses secure digital trade across the entire value chain.

However, if countries decide to move away from these standards by creating their own distinctive, bespoke regulations, then this makes it much harder for those taking part in digital trade to protect their businesses from cyberrisks. Regulatory divergence around cybersecurity requirements risks disrupting all of businesses' other efforts to secure digital trade and protect their clients, customers and operations.

The UK should work towards more coherent global standards on cybersecrutiy by using Free Trade Agreements to secure commitments from international partners to strengthen collaboration on identifying and countering cyberthreats and to recognise the benefits of a risk-based approach to cyberrisks over a prescriptive regulatory approach. The UK should try to mirror the commitments made on cybersecurity issues in the US-Mexico-Canada Trade Agreement (USMCA) and the US Japan Digital Agreement in its other FTAs, and work to include similar provisions in a WTO e-commerce agreement.

13 "Agreement" on a new Privacy Shield: Schrems III in the making? (Lexology, April 2022), Available at: https://www.lexology.com/library/detail.aspx?g=24fe34ab-23cd-493d-b8ac-f09aca5c380e

14 The ECJ decision in Schrems II rendered the EU-US Privacy Shield (a mechanism for transferring data from the EU to the US) invalid because US-based businesses could not guarantee that the US government would not be able to access the personal data of European citizens. SCCs were developed by the European Commission as possible alternative to the Privacy Shield – but it is not clear that they will survive further scrutiny by EU Courts.

What solutions should the UK adopt to grow digital trade and strengthen its competitiveness as a global data hub?

The following section sets out some policy solutions that could alleviate the operational frictions identified above. These are divided into three categories:

- **Policy changes the UK can make by itself to become a stronger global data hub**
- **Policy changes the UK can agree bilaterally with key trade partners to ease data flows**
- **Policy changes which can only be realised through global co-operation**

The UK needs to pursue policy change at all three levels simultaneously, working with industry to ensure that its approach is grounded in a proper understanding of operational realities.

The end goal should be a global agreement that enables "data free flows with trust", as was envisaged by the G20 in its Osaka declaration of 2019.[15] While this paper sketches what a comprehensive global agreement on data might look like, it recognises that it is unlikely in the short term, and unlikely to be achieved in one step.

Nonetheless, a global solution is, in the long term, the only sensible way of managing international data flows. The UK should work towards securing such an agreement and target domestic and bilateral data policy so that it supports this goal. The UK should model what a sensible global digital regime should look like in its own laws and work with industry and like-minded countries to scale similar solutions internationally.

While the main frictions affecting digital trade can only be resolved by government action, there is still much that industry should do by itself to further digital trade, including:

- **Creating new technology solutions that enable digital trade:** The private sector should design RegTech solutions to help businesses navigate regulatory divergence. New technologies are helping anonymise data taken from retail financial operations in different countries (e.g. to disguise credit card numbers) so that data can be transferred across borders more easily. If current levels of regulatory divergence continue, current business models are unlikely to be sustainable for long.[16] Technological solutions might become even more necessary to enable businesses to provide core functions.

15 Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows | World Economic Forum (weforum.org)

16 See, for example, A paper from the Institute of International Finance: STRATEGIC FRAMEWORK FOR DIGITAL ECONOMIC COOPERATION (April 2022), which points out that: "We are rapidly reaching an inflection point where data localization requirements and fragmented standards for data and privacy may begin to break the on demand services and real-time systems that we have come to expect and rely on." https://www.iif.com/Publications/ID/4879/Strategic-Framework-for-Digital-Economic-Cooperation--A-Path-for-Progress

- **Advocacy:** Only businesses can articulate the commercial necessity of digital trade and explain how digital protectionism will deprive businesses and consumers of choice, competition and high-quality digital services. Industry needs to continue to work with governments and regulators on a country-by-country basis, and at international institutions, to provide in-depth arguments for how each government, country, business community, population would benefit from data free flows, and lose out from data localisation. Businesses need to do more to explain to governments how tools such as cloud encryption keys can protect citizens' sensitive data.

Policy changes the UK can make by itself to become a stronger global data hub

Different jurisdictions play different roles within global digital trade networks. India, for example, has developed a competitive advantage for low cost, high-skilled English language technology expertise. Given its competitive advantages in financial and related professional services, the UK could position itself as a global data centre in these sectors – the natural location for businesses seeking to develop new FinTech, AI and blockchain applications.

To achieve this, the UK should make targeted changes to its data framework to ensure that businesses can store, process and access data in efficient and commercially sensible ways.

UK data policy should ensure that UK-based businesses can benefit from data connectivity, store data effectively, and be able to extract value from that data, including by analytics services. Some steps the UK can take to facilitate this include:

Provide guidance to businesses that illustrate how they should handle data that is on the borderlines of being personal and non-personal

The UK Data Protection Act distinguishes between personal data and non-personal data. It would be helpful for businesses to have access to clear guidance, based on practical examples and use cases, that articulates at what point in the data lifecycle a particular data point is treated by regulators as personal data or non-personal data.

It would be helpful if this guidance could provide examples that illustrate how anonymised personal data needs to be before it is seen as no longer personal. For example, it might illustrate when companies tracking financial crime can treat telephone records as being non-personal data – this will help facilitate investigations.

The UK government and data regulators could consult with industry to frame Codes of Conduct that set out such guidance. Industry is ready and willing to support regulators in framing such guidance. The long-term goal should be to secure buy-in to this guidance (or else deference to it) from key international governments and regulators. In this way, the UK could help scale-up a new, more context specific approach to data regulation.

Provide more guidance to financial institutions on the circumstances in which they can share personal data with other financial institutions to prevent crime

When financial institutions have identified someone as a potential financial criminal or money launderer, they are

currently often unsure how far data regulations permit them to share that information with other financial institutions to prevent further crime.

A bank might be able to take steps to protect itself against criminal activity, but not know whether it is allowed to warn others before it is too late. For example, it might suspect one of its customers of financial crime and want to share information about their IP address with other banks. However, the bank might be wrong in its suspicions and mistakenly share the IP address of an innocent customer with another bank. Banks need to share data about customers with each other to track financial crime and are often unsure how far they can share such information. The Data Protection Act states that there is a "legitimate interest" for financial institutions to share personal data to detect and prevent fraud. But it would be helpful if the ICO could give more explicit guidance to banks that explains that instances such as the above are occasions when firms can share data without breaking the rules. The ICO already helpfully provides examples of how insurance companies can process personal data to spot fraud.[17]

Create an information bank that enables UK businesses to conclude more commercial partnerships with non-EU technology providers

All businesses transferring personal data from the UK to non-EU markets must use Transfer Risk Assessments (TRAs) to set out how risky they think it is to transfer such data to their chosen jurisdiction. TRAs need to draw upon different kinds of information: some information (e.g. information about their business partners and data suppliers) is unique for each business.

But much information in TRAs is common to all businesses, such as information about the levels of personal data regulatory protection offered by different jurisdictions around the world. At the moment, all businesses need to make their own individual evaluations of such common risk profiles: this is inefficient, time consuming and costly. It also makes it hard for UK businesses to negotiate contracts with partners outside of the EU, depriving UK consumers of choice, competition and access to the best possible technology solutions.

If the UK government provided an information bank which provides data to inform the objective risk assessments of different countries' regulatory standards, businesses could access this as a shared resource and draw upon this when compiling their TRA responses. This would make it easier for UK businesses to work with a wider range of international business partners, cut the time that needs to be spent on onboarding new clients, and smooth contractual negotiations with US and Asian technology providers.

An alternative way of achieving the same goal might be for the UK government to help the financial and related professional services industry form a joint public-private information bank that covers the regulatory risks of transferring data to other countries; industry firms could all access, use, and update this shared resource. In this way, government could provide a platform that enables firms to work together to alleviate data frictions.

17 See, for example: What is the 'legitimate interests' basis? (ICO). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

Avoid domestic localisation measures

The UK has committed to avoiding unjustified data localisation in Free Trade Agreements and has taken a firm stance on the importance of free data flows with trust in international forums like the G7, G20, OECD, and WTO. But the UK needs to be careful to avoid undercutting its global advocacy by adopting data localisation measures at home.

In early proposals around the implementation of the Telecommunications Security Act 2021, for example, UK regulators considered requiring that network providers must operate a UK-based network - and monitor and audit it from the UK. UK regulators are currently reviewing these proposals.

There may be a justification for localisation in some cases, but the UK should avoid localisation where possible and adopt a whole-of-government approach whenever considering adopting it because of the major implications that any domestic localisation measures could have for UK trade policy internationally. The UK should make sure that any localisation measures are clearly stated, accessible for businesses, and adequately justified.

Ensure UK digital trade infrastructure is fit for purpose

The UK cannot take its digital infrastructure for granted. International financial centres rely upon the rapid exchange of information and need to be well embedded within global communications networks. Beyond trade and economic considerations, having strong and resilient digital infrastructure and the ability to defend it against cyberattacks is a critical national security priority.

The UK needs to upgrade both its domestic digital infrastructure by ensuring ultrafast broadband[18] and ensure that the subsea cables that form the bulk of its international digital infrastructure are equipped to handle more digital trade and resilient against global cyberthreats.

The US government reviews US subsea cable resilience every two years to ensure it is adequate for the country's needs: the UK government should do the same. As satellites increasingly look set to replace subsea cables as the primary conduit for international data flows, the UK also needs to ensure that its satellites are resilient against emerging space risks such as increasing collisions with debris and astropolitical risks including missile attacks on satellites.[19]

The UK should work with key allies when conducting reviews of its digital infrastructure. The government should publish findings on the resilience of the UK's digital infrastructure and whether it is fit for purpose given the UK's role as a leading global business hub. Government should also publish any recommendations on how to strengthen the UK's digital infrastructure.

18 See, for example, analysis that shows that UK broadband speed is slower than that in all other major international centres, set out in *Our global offer to business: London and the UK's competitive strengths in a critical time* (City of London Corporation, January 2022). Our global offer to business (theglobalcity.uk)

19 Global Risks Report 2022: Worlds Apart (Marsh McLennan, January 2022). Available at: https://www.marshmclennan.com/insights/publications/2022/january/global-risks-report.html

Policy changes the UK can agree bilaterally with key trade partners to ease data flows

While working towards a global agreement on data flows, the UK should engage bilaterally with trading partners to shape more open digital trade policies. The UK should:

Adopt a nuanced approach to addressing localisation

Industry strongly believes that data localisation is a mistake – a policy that imposes additional costs on consumers while restricting choice and competition. Industry opposes unjustified localisation measures, and urges the UK government to secure commitments from other countries to avoid such measures where possible. However, many countries have already implemented localisation laws or are in the process of doing so. While working to build a coalition of countries that favour digital trade, the UK should develop a nuanced approach to countries that are determined to localise.

The UK's approach to dealing with such countries will need to be context specific, but some overarching principles to inform policymaking should be:

1. **When a country is seriously contemplating localisation, the UK should urge it to avoid the most damaging kinds of localisation**

   Not all localisation measures are the same. A requirement that local citizens' data should be held on local servers is different to banning the processing and exporting of offshore data. If a country that is widely used as a data processing centre is considering localisation, it will be more damaging if it restricts the movement of offshore data than the movement of its own citizens' data. The UK's priority should be to minimise restrictions on offshore data.

2. **When a country is determined to localise, the UK should urge it to consider allowing local data to flow freely to some trusted markets, even if not all markets**

   Local authorities might not want local data to be stored on cloud based servers in every market, but they might trust some overseas jurisdictions enough to allow local data to be stored and processed there. In such cases, it would be better if regulators could partially localise, and only allow data to flow to a limited range of markets, rather than fully localise and not allow data to flow outside of their market. For example, a country might permit data to flow to trusted partners (e.g. close neighbours) but not elsewhere. Financial and related professional services businesses and cloud providers tend to operate their data storage services on a regional basis (i.e. one server in ASEAN, one in MENA, one in China, one in India). If businesses could use one of their regional servers to cater for a particular market, then this could provide for a compromise solution.

3. **When a country has imposed localisation laws, the UK should urge it to provide businesses with targeted exemptions to localisation measures**

   Even some countries that have adopted localisation rules have permitted financial institutions to move data out of the market for specific purposes (e.g. fighting financial crime and cybersecurity) where there is a vital need for a business to be able to draw on an integrated data set. Therefore, when a country has imposed localisation measures, the UK should consult with financial and related professional services businesses operating in that market to understand what data sets they really need to move out of the market. The UK should then work with local regulators and authorities to see whether clear and well-defined exemptions to the general localisation rules might be possible.

Use Free Trade Agreements (FTAs) to secure ground rules for digital trade

FTAs can establish ground rules for digital trade by including commitments to avoid unjustified data localisation measures (including localisation measures for financial data), enable cross-border data flows, and prevent customs duties from being imposed on e-commerce. FTAs can also include commitments to protect confidential information relating to software, source codes and encryption technologies. The UK should pursue bilateral commitments along these lines with all FTA partners.

However, the UK should be aware of the limitations of FTAs for securing digital trade. FTAs might create a policy environment more conducive to digital trade, but they cannot ensure it. Most digital trade chapters in FTAs still give signatories much freedom to impose localisation provided it is justified on public policy grounds. FTA digital trade chapters are a starting point for efforts to secure data free flows with trust, not a satisfactory conclusion. A forthcoming report, from The City of London Corporation, The Practical Implications of Digital FTA Provisions on the UK Financial Services Sector, sets out some detailed suggestions for how to leverage FTAs to secure digital trade given these limitations. The report suggests using trade negotiations as an opportunity to conclude digital Memoranda of Understanding between data regulators.[20]

Conclude financial data connectivity agreements:

Some countries have urged that financial data should be treated differently to other kinds of data, and exempted from FTA provisions that urge the free flow of other kinds of data. The UK should urge that financial data be treated in the same ways as other kinds of data. Regulators should be able to secure access to financial data when needed, but this does not mean that financial data should not be free to flow across borders in the same way as other data. One way in which the UK can build support for the notion that financial data should flow freely is by concluding financial data connectivity agreements with key trade partners. A model for what such agreements might look like is provided by the

20 "The Practical Implications of Digital Free Trade Agreement Provisions on the UK Financial Services Sector" (The City of London Corporation, publication date forthcoming)

United States-Singapore Joint Statement on Financial Services Data Connectivity (2020)[21] and the Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore (2020).[22] These agreements included commitments that authorities would work to ensure that financial service suppliers could transfer data, including financial data, across borders by electronic means and oppose the localisation of financial data. As with FTA commitments on digital trade, financial data connectivity agreements have some limitations, in that they contain public policy exemptions that allow countries to restrict data flows. However, financial data connectivity agreements provide some degree of reassurance to businesses that governments support the free flow of financial data.

Extend data adequacy to countries that share similarly high data protection standards

The UK could make it easier to transfer personal data across borders by declaring the data protection regime of other countries that offer high data standards "adequate". This would involve UK regulators declaring that the other country has sufficiently strong data protection standards that the UK thinks it is safe for businesses to move personal data there without SCCs or BCRs.

The UK should continue to explore adequacy declarations with its declared priority markets for adequacy - including Australia, South Korea, New Zealand and Singapore. If regulators feel that the data protection standards in these markets are sufficiently strong, they should move ahead with adequacy declarations provided they are mutually agreed.

Such adequacy measures could strengthen the competitiveness of the UK's International Financial Centre by making it easier for international financial institutions with relatively small UK offices to operate efficiently in the market. For example, if the UK declared Australia's data protection adequate, Australian bank branches in the UK might find it easier to share their trade and data with their headquarters in Australia, and thus be incentivised to grow further in the UK and open new of business lines in the UK market.

However, adequacy decisions should only be made when UK regulators are confident that the counterpart country shares high data protection standards. If the UK declares countries with weaker protections adequate, then other countries who currently consider the UK's data protections adequate (mainly but not exclusively the EU) may lose confidence in the UK's data regime and restrict frictionless data transfers to the UK. This would increase digital trade barriers and thus defeat the purpose of making adequacy declarations.

In practice, most financial and related professional services businesses do not rely much on adequacy agreements other than the UK-EU adequacy agreement. Therefore, the main benefit of the UK expanding adequacy decisions to other countries will probably not be that digital trade will rise in the short term. Rather, as the International Regulatory Strategy Group (IRSG) has noted, the most important reason for recognising more countries as adequate should be "to build a community where the essential role of data flows for the operation of financial services and the digital economy is recognised".[23] That is, the UK should use adequacy agreements to help shape a coalition of countries that support free data flows with trust. By signalling that it trusts regulators who are achieving high data protection standards, the UK will model the approach it would like other countries to adopt.

Use regulatory dialogues to ensure good regulatory practice on digital issues

The UK should conclude bilateral agreements with international regulators in which both countries commit to provide transparency around digital regulation and clear guidance on digital regulation. The UK should seek to get international regulators to agree to set out a timeline in which they will identify and publish all their countries' localisation (and soft localisation) requirements. The aim should be to encourage a culture in which regulators need to justify localisation measures. In such a climate, regulators would be more likely to consider alternatives to data localisation, and businesses would be given time to make representations to regulators on what these alternatives might be.

Whenever the UK and trade partners conclude data regulatory agreements (adequacy decisions or otherwise), they need to ensure that the ensuing regulatory guidance is accessible and user-friendly; otherwise, firms need to rely on lawyers to understand new rules. In Japan, for example, financial services businesses struggled to identify whether, following the UK-Japan adequacy decision, regulators still believed there was a clash between UK and Japanese regulations on biometric data. Without clear guidance, businesses needed to consult lawyers, despite the fact adequacy agreements are meant to reduce such frictions.

Digital trade liberalisation unaccompanied by user-friendly guidance about what has been liberalised is trade liberalisation in name only.

Secure international regulators' commitment to providing a secure portal through which businesses can provide regulators with encrypted information

Businesses increasingly use encryption to share confidential information in a secure manner. But often regulators do not accept encrypted documents from businesses, or at offer a safe portal through which confidential documents can be shared with them. This means businesses often need to share data with regulators in an unsafe way, defeating the purpose of many data protection regulations and raising operational risks. The UK should use international regulatory dialogues – especially dialogues with key trade partners - to urge international regulators to accept encrypted documents.

21 MAS-UST Joint Statement on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity

22 MAS-BSP Joint Statement on Data Connectivity: https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas

23 The future of international data transfers (IRSG, April 2022). Available at: https://www.irsg.co.uk/publications/irsg-report-the-future-of-international-data-transfers/#:~:text=As%20the%20pace%20of%20technological,%2C%20political%2C%20and%20societal%20scrutiny.

Policy changes which can only be realised through global co-operation

The ideal solution for the digital trade frictions identified in this report is a binding global agreement that enables "data free flows with trust".

Data flows cannot sensibly be regulated on a national basis. Regulating data is, in some ways, like regulating the sea. Countries can regulate their own nautical territory, but most seas lie beyond it. The UK can regulate a ship in the UK; Singapore can regulate it in Singapore. But whose rules do sailors follow when sailing from one to the other?

A national approach to regulating maritime commerce does not work. Over time, countries stopped trying to export their own standards by building maritime empires and agreed on common principles to govern maritime commerce. If they had not, today's businesses might have needed to comply with 193 different sets of maritime rules.

In the same way, while the UK can regulate data in the UK, and Singapore can regulate data in Singapore, no country can efficiently regulate the data moving between the two.

At the moment, however, more and more countries are trying to shape their own unique data regulations. If global trade is not to sink as businesses soon become compelled to reconcile 193 separate data regimes, all governments need to make a similar effort to devise common global data standards.

A global agreement might start as a scaled-up version of what the UK, US, Japan, and others have achieved in digital trade chapters of FTAs. But to really help businesses, it would need to go much further and set out the terms by which regulators could recognise each other's data regulations.

One model for such co-operation, as has been suggested by the International Regulatory Strategy Group, might be to stipulate that regulators should agree to recognise each other's data protection standards if regulators could demonstrate an adherence to Council of Europe Convention 108 standards on data protection or the OECD Privacy Principles and Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[24]

Given current global political realities, a global agreement on digital trade seems unlikely in the short to medium term. But there are tools at hand to start building one, and the UK should seize them:

Securing WTO E-Commerce agreement on the global ground rules of digital trade

The World Trade Organization's Joint Statement Initiative (JSI) on E-Commerce provides the most promising forum for securing global agreement in which bilateral FTA rules can be scaled globally. 71 WTO members (including the UK, US, EU, and China) are taking part in the JSI to negotiate ground rules on digital trade.

Negotiators have already provisionally agreed rules to support digital trade facilitation by developing common rules for approaching unsolicited commercial messages; e-signatures and authentication; e-contracts; open government data and online consumer protection.[25]

More challenging negotiations on data localisation are due to take place later in 2022. The UK should continue to work towards securing strong ground rules that limit unjustified localisation in all kinds of data – including financial data – in the final WTO agreement. At the moment, only the UK and the US support treating financial data in the same way as other kinds of data in the WTO E-Commerce talks – the UK needs to encourage others to support this position.[26]

The UK should also resist the temptation to secure a relatively easy, low value "early harvest" WTO agreement that only address digital trade facilitation and fails to tackle the most important digital friction of all - data localisation.

Creating a global agreement that enables the mutual recognition of data regulation

Even in the best-case scenario, a globalised version of UK FTA digital trade chapters concluded at the WTO could only provide global digital trade ground rules. It could not prevent digital regulatory fragmentation. It is a necessary but not sufficient solution to ensure data free flows with trust.

The UK needs to work towards a deeper kind of global agreement under which as many countries as possible agree on the principles by which they will recognise each other's data standards.

Exactly what these global principles might include would need to be agreed by participating countries during negotiations. One starting point might be to consider the proposition that all countries should recognise the data protection frameworks of countries whose data protection regime can be demonstrated to align with the Council of Europe's Convention on Data Transfers (Convention 108). Convention 108 strongly resembles the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (last updated in 2013). Since the OECD convention only covers personal data, it would be necessary to find ways of making its principles more flexible so that they could cover both personal and non-personal data.

Regulators from different countries might reject this starting point and propose alternative terms on which countries could recognise each other's standards. The ideal result would be for regulators to agree on some common terms for co-operation and standards for assessing whether countries' regulatory regimes attain those standards.

In the short term, an agreement along these lines between all countries looks highly unlikely. But a high degree of global consensus is not necessary. Most global agreements were not concluded in one step; rather, coalitions of willing countries shaped agreements which other countries signed up to over time. This approach ("plurilateralism") offers the best approach to get agreement on the mutual recognition of data regulation.

24 ibid

25 E-commerce Governance: Back to Geneva? (Centre for International Governance Innovation, February 2022), Available at: https://www.cigionline.org/articles/e-commerce-governance-back-to-geneva/

26 According to a leaked draft WTO text: wto_plurilateral_ecommerce_draft_consolidated_text.pdf (bilaterals.org)

This paper has pointed out many examples of global divergence in data standards. But some more promising countervailing trends towards convergence can also be detected. The EU's data protection regime, GDPR, is forming the basis of one kind of international data standard. The EU has extended adequacy to countries like the UK, South Korea, Japan, New Zealand, Canada, Argentina, Uruguay, and Israel on account of the similarity of these countries' data regimes to EU standards. Other countries such as Brazil have adopted data policies influenced by GDPR.

At the same time, the US, Japan, Singapore, Canada, South Korea and the Philippines have established the Global Cross Border Privacy Forum (Forum) to seek global interoperability of data standards. Forum members are considering recognising each other's rules if each country can demonstrate adherence to the APEC Privacy Framework.[27] The Forum is open to all countries that wish to join, and members have expressed eagerness for the UK to join.[28]

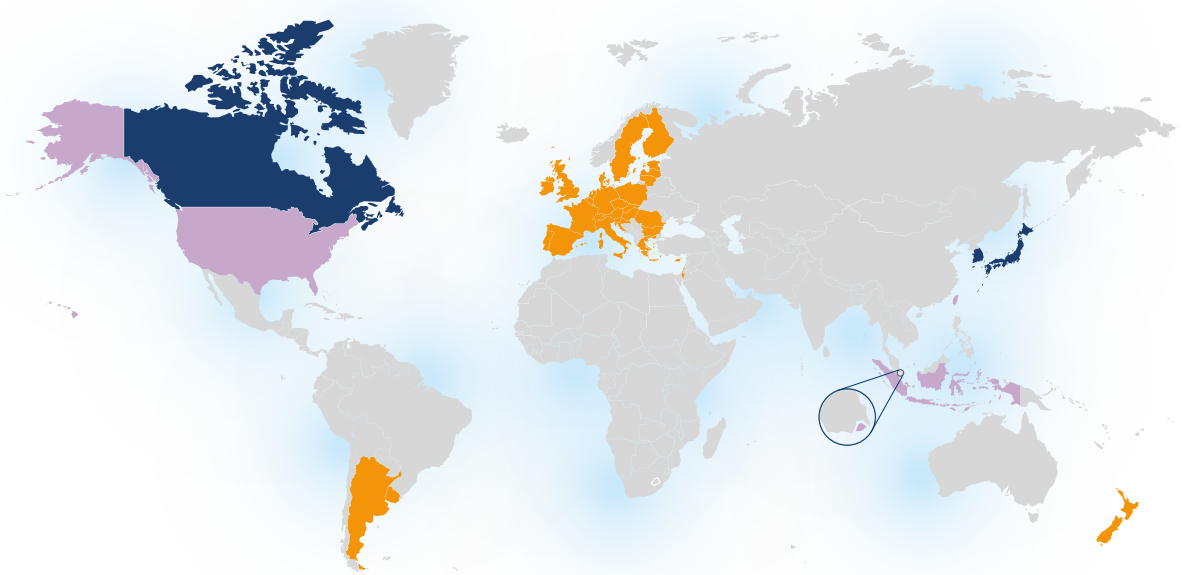
The UK should explore how it can work with Forum members to advance global data interoperability. From a UK business perspective, there are some difficulties with the Forum's current approach: Forum members have so far focussed only on private sector data flows (but public sector data needs to be covered too) and the APEC Privacy Framework is some way from the UK's EU-influenced data standards.

The UK should explore with Forum members, including members who also benefit from EU adequacy agreements like Japan, Canada and South Korea, to see if there are ways in which the Forum can reach an understanding with the EU on data flows. An agreement between the two parties on data flows could be the start of a global data agreement.

27 US Commerce Dept. announces 'historic' Global CBPR Forum for data transfers (IAPP, April 2022), Available at: https://iapp.org/news/a/us-commerce-department-announces-historic-global-cbpr-forum-for-data-transfers/

28 Washington goes on the global data privacy offensive (Politico, May 2022). Available at: https://www.politico.eu/article/washington-data-privacy-global-rules-restrictions/

Figure 4: Different Global Data Regimes



GDPR adequate (European Union, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, UK, Uruguay)

Forum member (The Philippines, Singapore, Taiwan, United States of America) **Both GDPR adequate and Forum member** (Canada, Japan, South Korea)

In the meantime, the UK should urge other countries that support open trade in data, such as the US, Japan, Switzerland, Canada, Australia, New Zealand, Chile, and Singapore, to work together to shape principles under which they would be willing to recognise the others' data regulations. Talks should be open to all who wish to join. Any agreement, once concluded, should be open to any other party that wishes to join. In this way, the approach of using mutual recognition to ensure data free flows with trust could scale and win more global support.

To provide governance for a new global agreement on data, there will need to be a new international institution to act as custodian to the agreement, provide a space for countries to discuss disputes arising under the agreements, and refine the agreements so they keep pace with technological change.

Participating countries would need to decide whether to set up a wholly new institution from scratch or create a new body that is linked to the structure of an existing international institution. The Organisation for Economic Co-operation and Development (OECD) has taken a lead on data regulation in the past and may be well suited to provide a Secretariat to a global data regulation body.

In recent years, many civil society organisations have called for a new set of global institutions to allow countries to agree on common approaches to twenty first century challenges and strengthen the rules-based international order.

The facilitation of data flows - so critical to global growth and global security and so hard to govern nationally – is a global public good challenge that needs to be resolved by a new global agreement backed by a new global institution. As the UK was at the forefront of efforts to shape our current global institutions, so now the UK should lead the charge to establish new agreements to solve new challenges.

Conclusion

This paper has demonstrated all of the ways in which digital trade is integral to the operation of financial and related professional services businesses.

The global success of UK-based financial and related professional services businesses in the last thirty years has been due to many factors. Undoubtedly the UK's position as a leading international financial centre has been key: businesses based in the UK have benefitted from deep pools of capital and talent, effective regulation, rule of law, flexible labour markets, an open trade and investment policy, an international language and a helpful time zone, and UK policymakers should continue to secure these factors to ensure future UK growth.

However, UK-based financial and related professional services have also succeeded because they have been able to take advantage of digital trade to build efficient global businesses that leverage data flows to ensure that customers and clients receive a high quality, secure service on a 24/7 basis. By operating such models, UK-based financial and related professional services businesses have been able to create a range of high-skilled UK jobs and generate a major contribution to UK economic growth.

The business models enabled by digital trade are now under threat from digital protectionism. In order to secure economic growth and enable job creation, the UK government needs to adopt policies that ensure that the UK remains as open as possible to data flows and work with trade partner countries to deliver bilateral and global agreements on data that achieve the G20 ambition of "data free flows with trust".

The UK-based financial and related professional services industry is ready and willing to work with governments and regulators around the world to deliver on this goal.

For more information on our digital trade work please contact:

Richard Hill, Manager, International Strategy, TheCityUK

+44 (0)20 3696 0128

richard.hill@thecityuk.com

TheCityUK

TheCityUK, Fitzwilliam House, 10 St Mary Axe, London, EC3A 8BF
www.thecityuk.com

MEMBERSHIP
To find out more about TheCityUK and the benefits of membership visit **www.thecityuk.com** or email us at **membership@thecityuk.com**

This report is based upon material in TheCityUK's possession or supplied to us from reputable sources, which we believe to be reliable. Whilst every effort has been made to ensure its accuracy, we cannot offer any guarantee that factual errors may not have occurred. Neither TheCityUK nor any officer or employee thereof accepts any liability or responsibility for any direct or indirect damage, consequential or other loss suffered by reason of inaccuracy or incorrectness. This publication is provided to you for information purposes and is not intended as an offer or solicitation for the purchase or sale of any financial instrument, or as the provision of financial advice. Copyright protection exists in this publication and it may not be produced or published in any other format by any person, for any purpose without the prior permission of the original data owner/publisher and/or TheCityUK.

© Copyright August 2022