CITY OF LONDON

FLINT

# The Practical Implications of Digital FTA Provisions on the UK Financial Services Sector

# Contents

# Foreword

The Financial and Professional Services (FPS) sector underpins prosperity across the UK and around the world. Firms' ability to sell services internationally is a key engine of jobs, growth and security.

As a global financial centre, the UK's international reach is unparalleled. Multinational FPS firms base themselves here to do business all over the world. In 2020, the UK was the largest global exporter of financial services generating a trade surplus of £63.7 billion.

Maintaining this position will require constant evolution. Technology is revolutionising global services trade and the FPS sector is already one of the most data intensive trading industries. These days, the ability of firms to transfer data around the world, and freely across jurisdictions, is as important as the ability to sell services and move people.

Yet we are seeing increasing examples of governments and regulators reacting to this technological revolution by restricting cross-border data flows. Whether this is the result of legitimate policy objectives or 'digital protectionism', these moves hinder digital services trade, driving ups costs for consumers and businesses, and ultimately threatening global financial stability.

We have welcomed the UK Government's prioritisation of digital trade in its international agenda to date. New free trade agreements (FTAs) with Australia, Japan and New Zealand, and the UK-Singapore Digital Economy Agreement, contain ground-breaking provisions facilitating cross-border data flows. In many ways, the UK is already setting the agenda.

More can be done. The UK Government needs to consider how its FTA agenda interacts with other policy mechanisms including regulatory diplomacy to encourage international cooperation on digital policy issues and, ultimately, deliver tangible benefits to firms. This report makes a series of recommendations for how UK Government should develop a more holistic approach to these issues to achieve genuine services trade liberalisation.

Success has never been more important. As we continue along the road to a post-Covid recovery, with global challenges including the Net Zero transition front of mind, and in the face of shifting geopolitical tensions, protecting and improving global FPS firms' capacity to trade across borders and provide services and capital to where they will deliver the greatest societal good will be a key determinant of success.

The City of London Corporation looks forward to this report contributing to and corralling the debate in this vital area. We look forward to working with UK Government and our many vital partners on these issues into the future.

**Chris Hayward**, Policy Chairman,
City of London Corporation

# Guest foreword

The UK's next generation trade deals aim to boost digital trade, prevent restrictions on the free flow of data, and unlock new commercial opportunities. Yet in practice, most policy makers and businesses struggle to articulate how and why free trade agreements facilitate cross-border movements of data and digital services.

We at Flint were delighted to work with the City of London Corporation on this report, which sets out how the UK financial services sector benefits from digital commitments in FTAs. We also welcomed the opportunity to propose practical improvements that, if implemented, could make digital trade commitments more commercially meaningful to financial firms.

That digital protectionism is prevalent in countries such as China, India and Indonesia is well documented. Of greater interest are new restrictions emerging in countries that traditionally advocate for cross-border data liberalisation such as the EU and the US. Given that many of these countries have committed to the free flow of data in free trade agreements, what has gone wrong?

Drawing on the UK's recent FTAs as case studies, our research demonstrates that digital commitments in free trade agreements come heavily caveated. Parties can, and do, fall back on national security, public policy, or prudential concerns to wriggle out of their trade commitments.

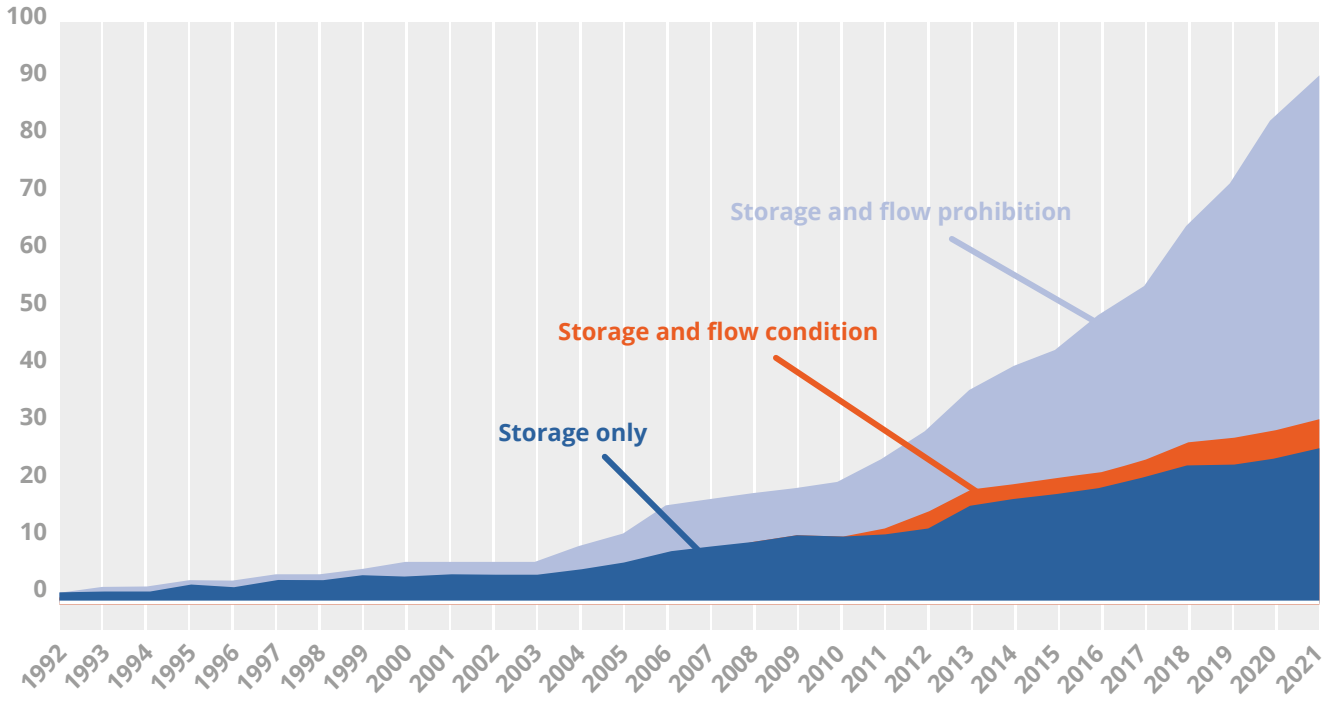
To deliver tangible economic benefits for financial services firms looking to trade internationally, the UK government needs to re-think its approach to digital trade. Regulators must be more involved during the negotiating process and take responsibility for delivering the outcomes, the scope of carve-outs and exceptions should be narrowed and refined to prevent abuse, formal mechanisms should be developed to allow firms to hold governments to account when they breach their digital obligations, and the UK needs to increase its efforts to facilitate the free-flow of personal data either via adequacy decisions or new policy mechanisms.

The UK is well-positioned to be a global leader on digital trade. But to do so, it must prioritise turning rhetoric and treaty commitments into new opportunities and tangible benefits for its companies.

**Sam Lowe**, Partner, Trade and Market Access Advisory practice, Flint Global

# Executive summary

**CHART 1:**
**FORCED DATA LOCALISATION OVER TIME**




**Source:** OECD, 'A Preliminary Mapping of Data Localisation Measures', 2022

- Barriers to digital trade are on the rise globally. The OECD has identified 92 explicit data localisation measures, across 39 countries.[1] The Information Technology and Innovation Foundation, a Washington-based think tank, estimates that explicit and implicit restrictions on international data transfers have more than doubled since 2017, with 144 now imposed by 62 countries. This includes over 40 measures that explicitly target financial, tax, and accounting data.[2]
- These barriers include behind-the-border regulatory measures that force firms to store and/or process data on local computer servers, apply duties to cross-border electronic transmissions, and condition market entry on the sharing of proprietary information such as source code.

1 OECD, **'A Preliminary Mapping of Data Localisation Measures'**, June 2022

2 Information Technology and Innovation Foundation, **'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them'**, Nigel Cory and Luke Dascoli, July 2021

- The UK is addressing barriers to digital trade through its free trade agreement (FTA) agenda. Its recent FTAs with Australia, Japan and New Zealand, and its Digital Economy Agreement with Singapore, all include ambitious digital trade provisions, and commitments designed to specifically facilitate cross-border flows of financial data.[3]
- This is especially important for the financial services sector. As the second largest global exporter of financial services (after the United States) the UK has a strong economic incentive to ensure its financial services firms can freely operate across multiple regulatory jurisdictions. In practice, this means being able to not only sell services remotely, but also to easily transfer financial data.
- There is little public, business, or political understanding of what digital trade provisions deliver in practice for the UK's financial services sector. Digital trade provisions rarely unlock new market access for firms – it is difficult to find a single example of one of the UK's new FTAs/ Digital Economy Agreements with Australia, Japan, New Zealand and Singapore leading to any of the countries allowing something that was not already permitted or changing an approach or rule they were not going to change anyway.
- The benefits of FTA digital provisions for financial services firms derive from them "locking in" pre-existing commitments to, for example, not require firms to store financial data on local servers or restrict the cross-border transfer of financial data. This provides additional certainty that firms will be able to continue operating on the same basis as now for the foreseeable future, and that liberalisation will not be withdrawn via discriminatory regulations.
- However, the additional assurances provided by FTAs are significantly undermined by a lack of government and regulator buy-in in practice, and a litany of carve-outs and exceptions. Regulators and governments can – and do – use public policy, privacy, prudential, regulator access and national security concerns to restrict the cross-border movement of financial data, despite headline FTA commitments not to do so. Even Australia, with its leading role supporting international data transfers and digital trade, makes it difficult for financial data (and health data) to be stored on cloud servers located outside of its territory.



**"There is little public, business, or political understanding of what digital trade provisions deliver in practice for the UK's financial services sector."**

3 Financial data is defined broadly in this report, capturing any data relevant to the day-to-day operations of a financial institution, for example payment and insurance data, and, in some instances, personal data.

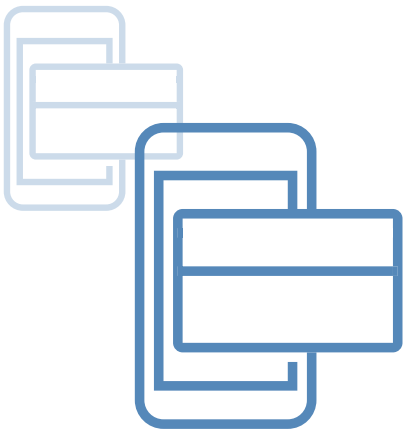
- As one of the few countries currently prioritising trade liberalisation, the UK is in a strong position to set the agenda on digital trade, and in financial services in particular. While countries and regulators will never forgo their right to regulate and intervene in an emergency, there are a number of actions the UK could take to ensure its digital trade commitments deliver tangible commercial benefits for financial services firms:

    1. **Involve financial regulators in defining negotiation terms and objectives.** Regulator engagement throughout the negotiation process – from the setting of the mandate to the implementation – would allow for a greater level of specificity in the negotiation and the direct linkage of trade provisions to existing and proposed regulatory interventions. Involving financial regulators to help develop the detail around their role within the agreement would also ensure that they have a vested interest in the full implementation of digital commitments, and increase their level of comfort with commitments made.

    2. **Build regulatory processes around specific concrete commitments.** Carve-outs and exceptions mean that there is little obligation on financial services regulators to accommodate new FTA commitments, or alter pre-existing approaches, unless they want to do so. Trade agreements should clearly outline the conditions applicable to financial data, provide clarity on how terms within the agreement should be interpreted by regulators and the parties, and be constructed in a way to limit the scope for de-facto data localisation.

       The UK-New Zealand FTA [Article 8.63] has constructive language limiting the exceptions on the free flow of financial data, placing a set of obligations on the party to undertake when looking to impose data localisation measures on a financial services supplier. However, for the terms to be meaningful and achieve their intended purpose, it is essential that partner countries and their respective regulators develop a shared understanding of what the various commitments mean in practice.

       New and existing FTAs should be supplemented by other trade policy tools such as joint regulator-to-regulator memorandums of understanding (MoU), as seen in the MoU between HM Treasury and the Monetary Authority of Singapore which provides for closer cooperation between the regulators and greater ability to share information between the markets.



**“Carve-outs and exceptions mean that there is little obligation on financial services regulators to accommodate new FTA commitments, or alter pre-existing approaches, unless they want to do so.”**

Amongst other things, digital MoUs could: commit the relevant financial regulators to reach and jointly publish a shared understanding of what constitutes a legitimate reason to order the onshoring of financial data; require the relevant counterparty regulators to identify, list and justify all pre-existing regulatory measures that could result in either the UK or its partner country breaching the FTA's digital trade commitments; compel the regulators to seek alternative solutions to localisation to achieve their objectives and impose a timely deadline on the relevant regulators reaching agreement on the above aligned with the respective FTA timeline.

3. **Include a formal mechanism for firms to escalate complaints.** UK FTAs, both future and current, should expand on the existing consultation provisions for financial services – which only allow governments to raise concerns – and include a consultation mechanism for relevant stakeholders and firms themselves. Such a mechanism should have a formal governance framework that sets the process for good faith engagement and structured escalation, allowing stakeholders to flag and challenge both existing and emerging concerns.
4. **Prioritise data adequacy.** Financial data is increasingly caught up in the rules governing, and restricting, the cross-border transfer of personal data. As per the recent International Regulatory Strategy Group report 'The future of international data transfers'[4], the ideal solution would be a global set of mutually acceptable principles that would underpin an international outcomes-based approach to privacy and the free flow of personal data. However, in the immediate term, the UK should prioritise its own data adequacy agreements with like-minded partners that UK regulators recognise have high standards of personal data protection. The agreements allow for personal data to flow more freely between the UK and covered third parties, facilitating the transfer of financial data and the associated economic benefits.



**"UK FTAs, both future and current, should expand on the existing consultation provisions for financial services – which only allow governments to raise concerns – and include a consultation mechanism for relevant stakeholders and firms themselves."**

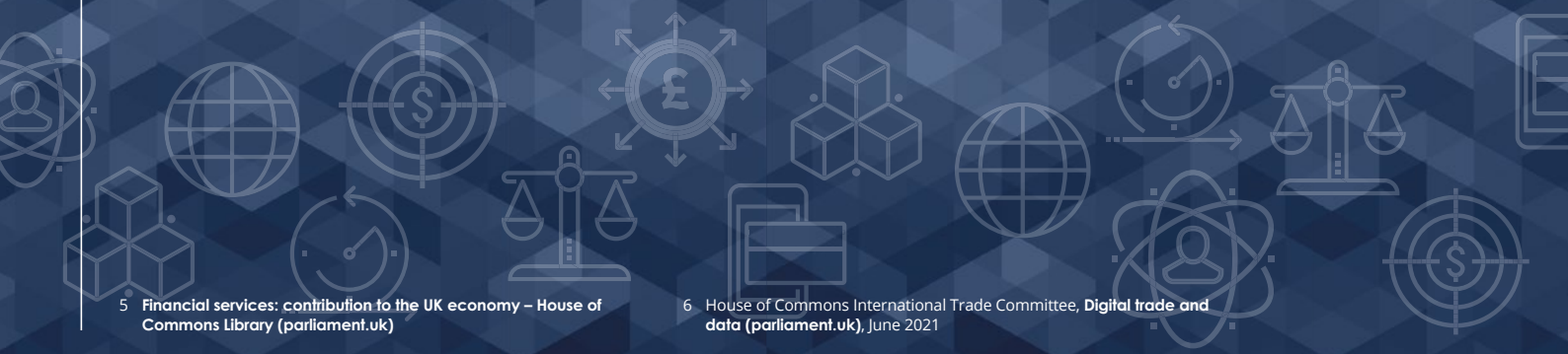
4 International Regulatory Strategy Group, **The future of international data transfers** | **IRSG**, April 2022

# Introduction

**Financial Services is one of the most data intensive trading industries. The ability to transfer data across jurisdictions is as important to financial firms as the ability to sell services and move people. Doing so allows them to more easily abide by regulatory obligations such as anti-money laundering and know-your-customer requirements, carry out and grow their international business operations, and provide value to customers.**

**The UK benefits significantly from financial services trade. In 2020, the UK financial services sector created 8.6% of total economic activity, was the fifth largest sector for the economy and was the third largest in the OECD by its proportion of national economic output, with exports worth £62 billion.**[5]

**The free movement of data across borders is integral to digital trade, the growth of the financial services sector and the ability of UK firms to grow internationally. The government itself has recognised that digital trade is dependent on the ability to move data across borders.**[6]



5 **Financial services: contribution to the UK economy – House of Commons Library (parliament.uk)**

6 House of Commons International Trade Committee, **Digital trade and data (parliament.uk)**, June 2021

However, governments and regulators are increasingly moving to restrict cross-border data flows. In the aftermath of the Global Financial Crisis, regulators across the world have made it harder for financial data to be stored and processed outside of their direct jurisdiction [**see Box 1**]. Geopolitical events such as Russia's invasion of Ukraine will only increase the frequency of political intervention.

Restrictions on cross-border data transfers are sometimes borne of legitimate regulatory or privacy concerns although often legacy requirements from a pre-cloud era. However, the rise of 'digital sovereignty' agendas, where countries (or blocs, in the case of the EU) prioritise national technologies to ostensibly increase resilience and reduce dependence on foreign technology, is leading to unnecessary restrictions on foreign providers (given they can use cloud services, for example, to provide data requested by financial authorities).

Restrictions include requirements for firms to store financial data on local computer servers, the application of duties to cross-border data flows and forcing firms to share proprietary information such as encryption algorithms with government and/or regulators as a condition of market entry.

The UK government has prioritised removing digital barriers to trade as part of its post-Brexit FTA agenda.[8] Recent UK FTAs with Australia, Japan, and New Zealand, along with a stand-alone Digital Economy Agreeement with Singapore, include ambitious digital trade provisions that commit to ensure the free flow of trusted data.

This paper will explore the impact of these digital trade provisions on UK financial services firms, with a particular focus on whether they succeed in unlocking any new day-one market access opportunities. It will then identify the limitations inherent to the FTA model as a tool to liberalise trade in financial services. Finally, it will propose several measures that the UK government could take to make the digital provisions in future FTAs more useful for the financial services sector.

> ***"Digital trade presents huge opportunities for our brilliant UK businesses, that's why we're building a global network of next-generation trade deals that drive productivity and boost high-paying jobs and growth in all parts of the UK.***
>
> ***By addressing digital protectionism on the global stage and championing a free, open, and competitive digital economy, more UK companies will be able to export their innovative, high-quality services and goods globally."***[7]
>
> **Anne Marie Trevelyan, UK Trade Secretary, 2021**

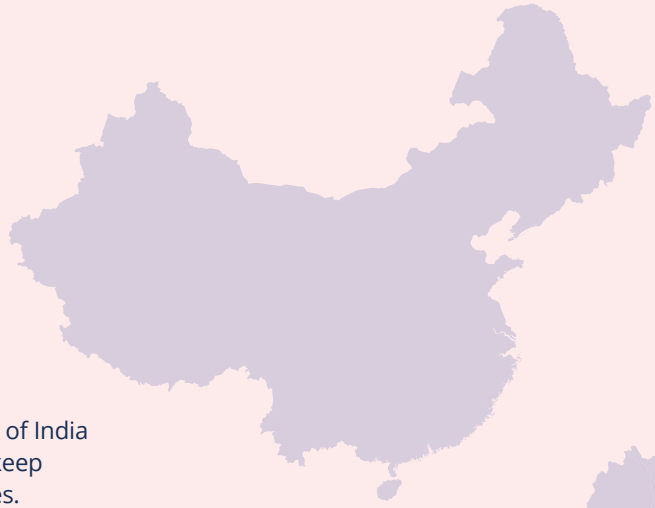
7 Department for International Trade '**Digital trade key to unlocking opportunities of the future**', November 2021

8 Department for International Trade, '**UK Digital Trade Plan**', September 2021

**BOX 1:**
**EXAMPLES OF RESTRICTIONS ON THE CROSS-BORDER TRANSFER OF FINANCIAL DATA**

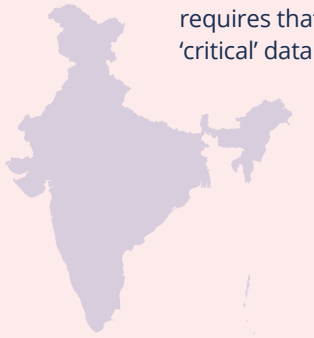
## China

Personal Financial Information, which is widely defined, collected or generated in China must also be stored and processed in China, affecting all banks, financial institutions and insurance firms. Personal data can only be transferred cross border in specific and restrictive circumstances.



## India

The Securities and Exchange Board of India requires that financial institutions keep 'critical' data within India boundaries.



## EU

A data project named 'GAIA-X' will create a European data cloud ecosystem in order to have digital sovereignty and reduce the use of US cloud providers throughout the bloc.

Further proposed EU measures (driven by France's cyber agency) would use cloud security standards to require firms to only use cloud services providers that are globally headquartered in the EU, majority EU owned and retain data within the EU territory.



## Indonesia

Despite regulations that allow firms to store data offshore, data localisation is de facto required under data policies for the financial and banking sectors.



## United States

In June this year, the US senate re-introduced a data export control bill which would create a new model to regulate the sale or transfer of US personal data to 'high-risk foreign countries'. If it passes, the legislation will create de facto data localisation measures on the premise of national security.



**Source:** How barriers to cross-border data flows are spreading globally, what they cost and how to address them, Information Technology Institute, July 2021; Reuters 2022

Section 1

# Why removing barriers to digital trade matters for UK financial services firms

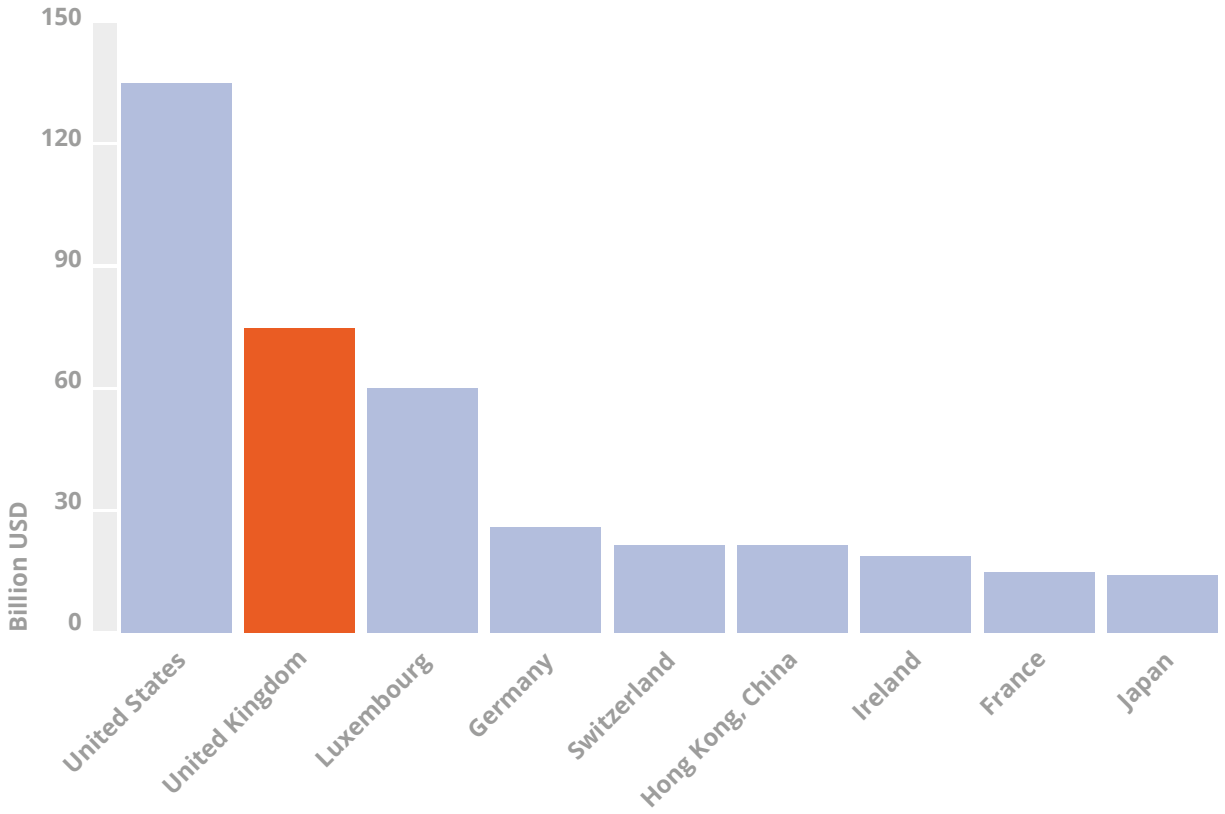
**The UK financial services sector is global in scale. As the second largest international exporter of financial services (after the United States), exporting £62 billion in financial services in 2020,[9] the UK has a strong economic incentive to ensure its firms can freely operate across multiple regulatory jurisdictions. In practice, this means being able to not only sell services remotely, but also to transfer financial data across borders.**

**But globally, barriers to digital trade are on the rise. The Information Technology and Innovation Foundation, a Washington-based think tank, estimates that data localisation restrictions have more than doubled since 2017, with 144 now imposed by 62 countries.[10]**

9 House of Commons, '**Financial services: contribution to the UK economy**', Georgina Hutton and Ali Shalchi, December 2021

10 Information Technology and Innovation Foundation, '**How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them**', Nigel Cory and Luke Dascoli, July 2021

**CHART 2:**
**TOTAL FINANCIAL SERVICES EXPORTS, 2019.**




**Source:** Authors calculation, OECD Stat.

**Digital trade barriers facing financial services firms include:**

- **Forced data localisation.** Requirements to store and process financial data on computer servers physically located within a given country erode the competitive advantage afforded by economies of scale. These measures impose a particularly steep cost on data-intensive industries.

  For example, local data processing, routing and storage requirements directly conflict with the value and purpose that cloud computing provides. Use of the cloud for data processing and storage has provided an opportunity for small and medium sized companies to conduct business beyond their border and access international markets where they would not have been able to previously.[11] While larger companies may be able to justify duplicating global processing and data storage functions to access a new market, smaller firms and start-ups are often unable to do so, stifling innovation and limiting their own market's access to new digital services and solutions.

  Data localisation can also create risks to global financial stability, as it reduces operational resilience by providing more points of entry for possible breaches of cybersecurity. It also limits the ability for markets to share data on IT system exposures to detect and respond to such attacks.

11 US International Trade Commission, **Policy Challenges of Cross-Border Cloud Computing**, Renee Berry and Matthew Reisman, May 2012

Not all data localisation is overt. Governments may also implement restrictions and requirements that make it significantly easier for companies to operate in-market if they store data locally even if they do not strictly prevent external processing and storage [**see Box 2**].

This results in growing and innovative companies being shut out of otherwise potentially lucrative markets, depriving them of potential growth and scaling-up opportunities. It also limits choice for consumers in those markets, blocking access to new financial products and services that would otherwise be available to them.

India, for example, poses a particular challenge for UK financial services firms. In 2018, citing the need for continuous monitoring and surveillance in order to reduce the risk of data breaches, the Reserve Bank of India directed payment firms to store all data related to payment systems on servers within India. Further data localisation measures could be enacted in India if and when proposed bills on personal and non-personal data protection that require copies of data to be stored within the market come into force.

- **Conditioning market access on the sharing of source code, cryptographic information and/or proprietary algorithms.** Some countries require foreign firms to share their source code, trade secrets or algorithms in order to access their market. China, in particular, has a history of requiring foreign firms such as Microsoft and IBM to share their source code with Chinese authorities.[12] Requiring companies to provide such commercially sensitive and confidential intellectual property raises concerns about secret, business-critical information being shared with domestic competitors. For financial services firms that engage in algorithmic trading, or rely on artificial intelligence, such requirements may constitute an intractable barrier to market entry.

- **Duties on cross-border data flows.** World Trade Organisation (WTO) members have agreed a moratorium on applying tariffs to electronic transmissions, which was recently extended at the 12th Ministerial Conference in June this year until the next conference, currently expected to be held in December 2023.[13] However, countries such as South Africa and India routinely threaten to veto the extension of the moratorium, meaning it cannot be relied upon in the long run. Were countries to apply tariffs to data flows, cross-border transaction costs for financial services firms would increase significantly.

**BOX 2:**
**CASE STUDY – SOUTH KOREA**

***South Korea has one of the world's strictest privacy regimes. Its personal information legislation mandates that financial services firms obtain the consent of South Korean data 'subjects' for all cross-border data transfers. Data subjects must be informed about who will receive the data, the purpose of the transfer, how long the data will be retained for and detail on the specific personal information provided.***

***Further obligations exist for financial firms storing data on the cloud. While South Korea's 2016 Regulation on Supervision of Electronic Financial Transactions now allow for the use of cloud services by financial firms, the Financial Services Commission specifically requires that providers processing personal information and identification data, such as credit scores, be located in South Korea.***[14]

12 Peterson Institute for International Economics, '**Should US tech companies share their "source code" with China?**', Theodore H Moran, October 2015

13 WTO Work Programme on Electronic Commerce June 2022

14 Lexology, '**Q&A: cloud computing law in South Korea**', LAB Partners, November 13 2020.

## Drivers of restrictions on digital/financial services trade

FTAs rarely liberalise trade in regulated services. Unlike trade in goods, traded services are not subject to easily quantifiable tariffs, which FTAs can remove or reduce. Rather, barriers to trade in services are borne of the wider domestic policy context and shaped by political preferences on issues such as immigration control.

While not conducive to global economic and commercial growth, some jurisdictions are reluctant to allow regulated services activity to take place outside of their legal jurisdiction. Unlike trade in goods, services regulators cannot rely on physical checks at the border to uphold their territory's regulatory integrity and ensure local rules are being obeyed.

Trade liberalisation can require regulators to trust not only that the relevant rules and regulations are being followed by a foreign firm, but also that if something goes wrong a foreign regulator or government will hold the firm to account. This creates a liability mismatch: foreign firms and regulators are tasked with upholding compliance, but domestic regulators and politicians will suffer the political fallout if something goes wrong. And in the case of citizen's personal information, or systemically significant economic activity, countries are often unwilling to take the risk.

The practical result of political and regulator hesitancy with respect to regulated foreign service providers is that countries usually find a way – either through local presence requirements, board nationality requirements, equity caps or professional qualification rules – to ensure these firms create and maintain a local presence as a condition of market entry.

Financial services firms face particularly burdensome market access barriers. Foreign financial services firms selling directly to UK consumers, for example, are usually required to set up a local branch or subsidiary. Where procedures do exist to facilitate cross-border financial services trade, such as the EU's equivalence regime, they are usually unilateral, allowing regulators to pull the plug at short notice, and often do not cover the full range of services a firm may seek to provide.

Beyond wider structural barriers to trade in financial services, specific concerns leading to barriers to the cross-border movement of financial data include:

- **Privacy**

  Edward Snowden's National Security whistleblowing disclosures in 2013 brought global attention to the issue of data security and privacy. While data localisation existed before the Snowden leaks, the fallout created a surge in measures from governments wanting to be seen to be doing something to protect citizens and business from data and privacy threats.[15] In Europe, a personal data sharing arrangement with the US – the so-called Privacy Shield – collapsed following a legal challenge and European Court of Justice ruling that the framework provided insufficient protection and privacy of EU personal data when transferred to the US.[16] The decision also created burdensome obligations for companies that move or process data between the US and EU when relying on Standard Contractual Clauses – requiring them to carry out case-by-case assessments of data protection, potentially expecting them to implement additional safeguards or stop high-risk transfers.

15 Jonah Force Hill, **The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders** 2014

16 Court of Justice of the European Union **Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems** July 2020

- **Regulator access**

  For financial regulators, the ability to access a firm's data in a timely fashion is key in order to supervise relevant data, to mitigate consumer harm and ensure data held in another location is not misused, to prevent regulatory arbitrage, and to maintain the integrity of the market's financial system. This has led many regulators to require companies to store financial data on local computer services, believing that doing so provides for greater security and access, particularly in the event of a crisis or financial crash.

  In the US, the collapse of Lehman Brothers in 2008, and the subsequent difficulties accessing data stored across multiple geographies and regulatory jurisdictions during the bankruptcy procedures, led the US financial regulatory agencies to advocate for, and achieve, a carve out for financial services data in the Trans-Pacific Partnership (TPP) negotiations. Of particular concern was the restrictions placed on data transfers by the UK regulator, following its takeover of Lehman's Europe division.[17] The specific issue of how data should be dealt with in the event of a global bank's demise has since been addressed through requirements for financial institutions to prepare "living wills", but regulator efforts to keep data within arm's reach persist.[18]

- **Protectionism**

  Digital protectionism can be both overt and/or a by-product of poorly designed rules and heavy-handed implementation. Some governments act to restrict the cross-border flow of data in the belief that local storage will result in growth opportunities for local business and talent. Nigeria, for example, explicitly requires ICT companies to host data locally to build capacity and equip Nigerians to "serve as active workers and participants in the local ICT industry'.[19]

  Digital protectionism is not solely the preserve of developing or emerging economies. Much of the language used by politicians in Europe to justify restrictions on the free flow of data centres on the belief it will create local jobs and create value. This is despite there being little evidence to support such claims. However, while there are legitimate reasons to restrict cross-border data transfers, in practice countries are routinely going far beyond what is strictly necessary to achieve their regulatory objectives, creating unnecessary cost and barriers to market entry for financial services firms.

**"Digital protectionism can be both overt and/or a by-product of poorly designed rules and heavy-handed implementation."**

17 Information Technology and Innovation Foundation, **Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements**, Nigel Cory and Robert D Atkinson, April 2016

18 Victoria L Lemieux, **Financial Records and Their Discontents** 2012

19 National Information Technology Development Agency (NITDA) **Guidelines for Nigerian Content in ICT** August 2019

Section 2

# What UK trade deals do for digital

**The UK is one of the world's premier services hubs, internationally recognised for its openness, global connections, and collaborative regulatory culture.[20] Ministers are therefore keen to highlight the opportunities new UK FTAs unlock for digital and financial services firms.**

**Since leaving the EU, the UK has signed new FTAs with Japan, Australia, and New Zealand, alongside a digital economy agreement with Singapore. These deals all feature ambitious digital provisions that go further than past agreements in their attempts to address issues specifically affecting financial services firms [see Annex 1]**

20 Department for International Trade, **UK and Singapore sign new innovative digital trade deal**, February 2022

**TABLE 1:**
**DIGITAL TRADE PROVISIONS IN THE UK'S FTAS**

| Digital Trade Provision | CEPA | UK Australia | UK NZ | UK Singapore DEA |
|---|---|---|---|---|
| Elimination of customs duties on electronic transmissions | YES | YES | YES | YES |
| Electronic Contracts | YES | YES | YES | YES |
| Electronic authentication and electronic signatures | YES | YES | YES | YES |
| Electronic Invoicing | NO | YES | YES | YES |
| Paperless trading | NO | YES | YES | YES |
| Domestic electronic transactions framework | YES | YES | YES | YES |
| Online consumer protection | YES | YES | YES | YES |
| Digital Identities | NO | YES | YES | YES |
| Measures against unsolicited commercial electronic communications | YES | YES | YES | YES |
| Cryptography | YES | YES | YES | YES |
| Personal Information Protection | YES | YES | YES | YES |
| Data Flows / Cross Border transfer of information | YES | YES | YES | YES |
| Prohibition of data localisation | YES | YES | YES | YES |
| Financial data flows/ cross border transfer of information | YES | YES | YES | YES |
| Prohibition of data localisation for financial services | YES | YES | YES | YES |
| Cooperation | YES | YES | YES | YES |
| Cybersecurity | YES | YES | YES | YES |
| Non-disclosure of source code and related algorithms | YES | YES | NO | YES |
| Open internet access | YES | YES | YES | NO |
| Open Government Data | YES | YES | YES | YES |

**Specific provisions include:**

- **Data localisation prohibitions.** The UK-Australia, UK-New Zealand, UK-Japan and UK-Singapore DEA deals include provisions specifically prohibiting the forced localisation of financial data and computer servers. The commitments are conditioned on the firm making available all necessary information for the purpose of financial regulation and supervision in a timely fashion. They are also subject to public policy, prudential and national security exceptions.

  This explicit prohibition on the localisation of financial data is modelled on the provisions found originally in the US-Mexico-Canada Agreement (USMCA) and go further than the catchall anti-localisation provisions of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economic Partnership Agreement (DEPA).[21]

> ***"This digital agreement plays to our strengths as a services superpower and will ensure our brilliant businesses can build back better from the pandemic and benefit from easier, quicker and more trusted access to the lucrative Singapore market.***
>
> ***We're using our independent trade policy to strike these groundbreaking agreements that create high-skilled, well-paid jobs across the UK – paving the way for a new era of modern trade."***
>
> **International Trade Secretary Anne-Marie Trevelyan, following the signing of the UK-Singapore Digital Economy Agreement.**[22]

21 The City of London Corporation and EY, The City of London: an ecosystem enabling international trade George Riddell and Duncan Richardson, May 2021

22 Visa Economic Empowerment Institute Trade agreements to move the digital economy Mike Gallaher, December 2020

**BOX 3:**
**UK-AUSTRALIA FTA ARTICLE 9.12**

**FINANCIAL DATA AND INFORMATION**

1. *The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means and the use of financial service computing facilities, including requirements that seek to ensure the security and confidentiality of communications.*
2. *Neither Party shall prohibit or restrict a financial service supplier of the other Party from transferring, including by electronic means, information including personal information, where those transfers are necessary for the conduct of the ordinary business of the financial service supplier.*
3. *Subject to paragraphs 4 and 5, it is prohibited for a Party to require, as a condition for conducting business in the Party's territory, a financial service supplier of the other Party to use or locate financial service computing facilities, in the former Party's territory.*
4. *Each Party has the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure appropriate access to information required for the purposes of financial regulation and supervision, provided that the following conditions are met:*
   - *(a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and*
   - *(b) the Party or its regulatory authorities inform the other Party or its regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.*
5. *Nothing shall restrict the right of a Party to adopt or maintain measures inconsistent with paragraph 2 or paragraph 3 to achieve a legitimate public policy objective such as the protection of personal information, personal privacy, and the confidentiality of individual records and accounts, provided that the measure:*
6. *(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information or on the use or location of computing facilities greater than are required to achieve the objective.*
7. *This Article does not apply to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection.*
8. *This Article does not apply to credit information, or related personal information, of a natural person.*

- **Restrictions on conditioning market access on the sharing of source code, cryptographic information, and proprietary algorithms.** The UK-Australia, UK-Japan and UK-Singapore agreements include provisions that prohibit the forced transfer of, or access to, source code, cryptographic information (such as private keys), and proprietary algorithms. New Zealand does not make specific commitments on source code, due to similar provisions in the CPTPP being found to breach its legal obligations to guard the "data sovereignty" of its Māori population.[23]

  These commitments are not unconditional. Explicit caveats ensure regulators and judicial authorities can access this information for the purposes of assessing conformity with local rules and law enforcement.

  Some UK FTAs contain exceptions within their source code provisions to ensure regulators have the discretionary power to carry out investigations. This can be seen in the UK-Japan and UK-Australia agreements where financial services regulators are not covered by the primary obligations of the article for the purpose of regulatory intervention. The cryptography provisions (Japan, Australia, New Zealand and Singapore) are more explicit: financial instruments, central banks, financial service suppliers and financial markets are specified as exceptions.

**BOX 4 :**
**UK-JAPAN CEPA ARTICLE 8.73**

**SOURCE CODE**

*1. A Party shall not require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.*

*2. This Article shall not preclude a regulatory body or judicial authority of a Party, or a Party with respect to a conformity assessment body, from requiring a person of the other Party:*

*(a) to preserve and make available1 the source code of software, or an algorithm expressed in that source code, for an investigation, inspection, examination, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure; or*

*(b) to transfer or provide access to the source code of software, or an algorithm expressed in that source code, for the purpose of imposing or enforcing a remedy granted in accordance with that Party's law following an investigation, inspection, examination, enforcement action or judicial proceedings.*

*3. This Article does not apply to:*

*(a) the voluntary transfer of, or granting of access to, source code, or an algorithm expressed in that source code, by a person of the other Party, such as in the context of a freely negotiated contract or government procurement; or*

*(b) services supplied or activities performed in the exercise of governmental authority.*

*4. For greater certainty, this Article shall not prevent a Party from adopting or maintaining measures1 inconsistent with paragraph 1, In accordance with:*

*(a) Article 1.5, Article 8.3 and Article 8.65; or*

*(b) Article III of the GPA, as incorporated by Article 10.1.*

23 Sam Lowe, Most Favoured Nation: The Treaty of Waitangi, Revisited March 2022

- **No customs duties on cross-border digital flows.** The UK-New Zealand, UK-Australia, UK-Japan and UK-Singapore agreements all contain commitments to ensure tariffs are not imposed on content transmitted electronically.

**BOX 5:**
**UK-NEW ZEALAND FTA ARTICLE 15.4**

**CUSTOMS DUTIES**

1. *Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.*
2. *For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions, including content transmitted electronically, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.*
3. *The Parties shall cooperate in relevant international fora to promote the adoption of commitments by non-parties not to impose customs duties on electronic transmissions.*

## NEW MARKET ACCESS?

The benefits of services provisions, and digital services provisions, in FTAs are misunderstood.

FTAs rarely unlock new cross-border market access opportunities for foreign regulated services providers. Prior to signing their FTA, neither the UK or New Zealand, for example, explicitly required foreign financial services firms to store their financial data on local computer servers, applied tariffs to cross-border data flows, or forced foreign firms to hand over their source code and proprietary data.

Rather, new FTA digital commitments attempt to clarify and lock in existing levels of applied market access or reflect measures governments were planning to implement anyway. This provides financial services firms with an additional reassurance that market access conditions will not be rolled-back in future. The specific treaty provisions also give companies an additional legal hook to hang their government and regulator engagement on when related issues do arise [**see Case Study 1**].

These reassurances can be of particular importance when operating in a country that is in the process of introducing new restrictions to digital trade. India, for example, continues to introduce a number of impediments to cross-border data flows. These include the 2018 banking mandate for all payment data to be stored within India, 2020 know-your-customer requirements that calls for the technology infrastructure to be housed locally, and proposed personal and non-personal data protection bills (now being re-considered) that would set out a nationwide data localisation framework whereby all data deemed 'sensitive' or 'critical' could not move freely out of India.[24] India also regularly threatens to renege on its WTO commitment and impose duties on cross-border data flows.

Digital provisions in a UK-India FTA, given the context, could provide a heightened level of reassurance for UK firms, and an advantage over those selling into India from other jurisdictions.

Progressive digital provisions within FTAs can also create new de facto global standards on digital trade, setting a standard benchmark that limits the use of data localisation and enables trusted data flows for like-minded countries to base future agreements on.

24 Carnegie Endowment for International Peace, How Would Data Localization Benefit India? Anirudh Burman and Upasana Sharma, April 2021

CASE STUDY 1:

# SINGAPORE AND NEW ZEALAND

*New Zealand and Singapore agreements reaffirm existing levels of openness but provide little in the way of new market access.*

### *NEW ZEALAND*

*The UK's FTA with New Zealand includes commitments prohibiting the forced localisation of financial data. This was welcomed by UK financial firms, claiming that the ability to move data freely between the UK and New Zealand markets would enable them to scale in the region.*

*However, New Zealand did not have any preexisting data flow restrictions or localisation requirements that restricted the cross-border flow of financial data from the UK – data can be transferred outside of New Zealand as long as a company ensures that the basic principles of the Privacy Act are complied with. There are some circumstances when approval is required from the Commissioner of Inland Revenue to store electronic business and tax records outside of New Zealand.*

*While New Zealand's Privacy Act does include restrictions on offshore transfers of personal information, the UK and New Zealand have an adequacy arrangement which largely overcomes this issue. Additionally, the use of an offshore data processor, such as a cloud storage provider, does not constitute an overseas disclosure under the Act, allowing companies to easily store data abroad (very few international firms house data centers in New Zealand).*

### *SINGAPORE*

*Following the announcement of the UK-Singapore Digital Economy Agreement in 2022, UK business groups welcomed the deal and its commitment to free data flows, including specific commitments covering financial data. However, these commitments do not go beyond what already existed at a regulatory level between the UK and Singapore. Singapore is an international commercial hub that relies on transferring data internationally with no real desire to make it difficult for data to flow outside its borders.*

*The UK and Singapore established the first FinTech bridge in 2016, allowing financial services firms to operate more efficiently in each other's jurisdiction. Singapore also grants digital banking licences, allowing some international companies, including 'non-bank players' to carry out digital banking businesses in Singapore.*

*Singapore's Personal Data Protection Act is already more flexible than other international data regulations, allowing for third party processing of data and less onerous conformity requirements for companies, with broader exceptions. The country has long recognised the value of data flows for trade, and is a leading player in the push to establish global data connectively.*

**"New Zealand and Singapore agreements reaffirm existing levels of openness but provide little in the way of new market access."**

Section 3

# Limitations

**FTA digital provisions are heavily caveated and subject to a number of carve outs and exceptions, creating a large degree of uncertainty for financial services firms looking for guidance. Regulators and policymakers need to find a balance that addresses the limitations of trade provisions whilst exercising regulatory control.**

There are also the wider financial services rules to consider. FTA provisions determining whether foreign financial services providers are allowed to enter a market (market access), sell into the market cross-border from a foreign territory, and be treated on equal terms to local firms (national treatment) are usually very limited.

The cross-border supply of banking services in respect of deposit taking, lending, trading, and the issuing of financial securities are not covered by UK FTA market access and national treatment commitments, for example.[25] This means that in practice there are already many restrictions and barriers preventing foreign-based financial services firms from operating in the UK, and its trade partner's market, even before considering the rules on digital and data.

Specific limitations on the effectiveness of digital trade provisions can crudely be placed into two boxes: carve-outs and exceptions.

## CARVE-OUTS

Digital FTA commitments are rarely unconditional, and usually heavily caveated. For example, the UK-Japan commitments to refrain from forcing financial firms to onshore their data contains the following carve outs [**bold**]:

### Article 8.63 Financial information

1. A Party shall not restrict a financial service supplier of the other Party from transferring information, including transfers of data into and out of the former Party's territory by electronic or other means, where such transfers are relevant for the conduct of the ordinary business of the financial service supplier.
2. Subject to paragraph 3, a Party shall not require, as a condition for conducting business in its territory, a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.[26]
3. **A Party has the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure access to information that is appropriate[27] for the purposes of effective financial regulation and supervision, provided that the following conditions are met:**

   (a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and

   (b) the Party or its financial regulatory authorities consults the other Party or its financial regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.
4. Nothing in paragraph 3 shall be construed to grant a Party access to information or to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, in a manner beyond what is appropriate for the purposes of effective financial regulation and supervision.
5. **Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as that right is not used to circumvent Sections B to D [commitments on investment, cross-border trade and temporary movement of people] and this Sub-Section.**

25 Annex 11A Cross-Border Trade in Financial Services, Schedule of the United Kingdom of the UK-New Zealand Free Trade Agreement, with cross-reference to Chapter 11, Article 11.1, for example.

26 UK Australia Free Trade Agreement Chapter 31 General Provisions and Exceptions

27 Wilson Center, **USMCA Data and Digital Trade Provisions: Status Check** Nigel Cory, November 2021

Another example is the caveat applied to the commitment not to apply duties to cross-border flows in the UK-Australia FTA [bold]:

**Article 14.3 Customs Duties**

1. Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.
2. **For greater certainty, paragraph 1 does not preclude a Party from imposing internal taxes, fees or other charges on electronic transmissions, including content transmitted electronically, provided that those taxes, fees or charges are imposed in a manner consistent with this Agreement.**

As well as the provisions highlighted, there is no agreed understanding of what words and phrases like *"ordinary business", "reasonable opportunity", "consult"* and *"appropriate for the purposes of effective financial regulation and supervision"* mean in practice.

These caveats and ambiguities provide signatories and their regulators with a large degree of discretion to determine whether to abide by the commitments, or not, with very limited governance around whether they are abiding by the commitments and call into question their commercial benefit.

## EXCEPTIONS

Digital provisions in respect of financial services can find themselves subject to three major exceptions: national security, prudential, and public policy (of which personal privacy is a component part).

- **National Security.** All FTAs, and trade commitments in the context of the WTO, are subject to a national security exception. This largely self-judging exception allows countries to breach their treaty commitments to apply "measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests" or to "access to any information the disclosure of which it determines to be contrary to its essential security interests".[28]

  The security exception is increasingly being used illegitimately to justify the introduction of trade restrictive, and discriminatory, data localisation measures. For example, despite USMCA committing parties to not force firms to localise financial data, Mexico has done just that due to alleged national security concerns.[29]

  Geopolitical events such as Russia's invasion of Ukraine will increase political pressure to restrict data flows on the basis of national security concerns.

- **Prudential.** Mirroring similar provisions in the WTO's Annex on Financial Services30, UK FTAs contain a so-called prudential carve-out. This carve-out allows regulators to breach UK trade commitments in respect of financial services if necessary to ensure financial stability, among other things [**see Box 6** for an example].

  In practice, the broad nature of the prudential carve-out provides cover for almost any action taken by a financial services regulator, and significantly undermines the binding power of all financial services-related FTA provisions. If a regulator wants to do something an FTA says it should not do – for example force a firm to store its data on local servers – the prudential carve-out provides a route for them to do so. The UK does not explicitly require financial firms to store data locally, but the overlap between its data privacy regime and anti-money laundering and know your customer requirements have a similar effect. Australia – one of the more instinctively liberal countries in respect of cross-border financial data flows – is an instructive example of how regulator unease can create de-facto data localisation requirements [**see Case Study 2**].

28 WTO Annex on Financial Services

29 Memorandum of Understanding between Her Majesty's Treasury and The Monetary Authority of Singapore on Financial Services Regulatory Cooperation

30 KPMG/ IRSG, The future of international data transfers, April 2022

**BOX 6:**
**UK-JAPAN FTA ARTICLE 8.65**

**Prudential carve-out**

*1. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures for prudential reasons, including for:*

*(a) the protection of investors, depositors, policy-holders or persons to whom a fiduciary duty is owed by a financial service supplier; or*

*(b) ensuring the integrity and stability of the Party's financial system.*

*2. Where such measures do not conform with this Agreement, they shall not be used as a means of avoiding the Party's obligations under this Agreement.*

*3. Nothing in this Agreement shall be construed as requiring a Party to disclose information relating to the affairs and accounts of individual customers or any confidential or proprietary information in the possession of public entities.*

**BOX 7:**
**UK-SINGAPORE DEA, ARTICLE 8.61-F**

**Cross-Border Transfer of Information by Electronic Means**

*1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.*

*2. Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person.*

**3. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:**

**(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and**

**(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.**

- **Public policy.** UK FTAs contain provisions allowing both parties to breach their commitments on cross-border data flows so long as the breach serves a legitimate public policy objective [**see Box 7** for an example]. This provision is broad and covers such interventions as those to uphold privacy and data protection, the protection of public health, the defence of public morals and the protection of cultural diversity.

  It is the public policy exception that, for example, enables the UK to retain General Data Protection Regulation (GDPR) and its restrictions on the free-flow of cross-border personal data despite having signed up to a number of agreements and provisions that on first glace are contradictory.

Collectively, the three major exceptions create considerable latitude for countries and their regulators to justify any breach of their commitments in respect of the free flow of financial data. The exceptions are not unique to UK agreements and are borne of a general unwillingness by governments to give up room for manoeuvre. All three exceptions are arguably necessary – no government should be constrained from acting in the event of, for example, being invaded, or during a financial crisis – but their broad application has historically led to abuse. The fact that Australia, the UK, and United States are unwilling to limit the scope of exceptions themselves provides a loophole for genuinely protectionist countries to misuse them. For example, China believes

it is able to comply with the substantial digital and data localisation prohibition provisions of the CPTPP, despite implementing a world-leading number of restrictions on moving data in and out of China, is a result of these exceptions, and should give trade policymakers pause for thought.

**CASE STUDY 2:**

## AUSTRALIA

*The UK Australia FTA contains provisions that expressly prohibit conditioning market access of financial data being stored on local computer servers. However, Australia's domestic financial regulatory regime in respect of outsourcing and cloud services provisions can, under certain circumstances, operate as a de facto localisation requirement, and prevent UK financial services firms from accessing the Australian market.*

*A UK tech start-up that provides biometric verification services to financial firms has faced issues when working within certain regulated sectors in Australia. The company engages an international cloud platform outside Australia, processing biometric identify information on a server that is also used for non-financial services clients.*

*Financial companies that are regulated by the Australian Prudential Regulation Authority (APRA) are required to consult with the APRA before entering an offshoring agreement with a non-Australian company. When APRA considers an arrangement to be of extreme inherent risk, the companies must demonstrate that their risk management and mitigation techniques are sufficiently strong to counter any threat. Companies that utilise public cloud arrangements for biometric identify data fall within the APRA's definition of extreme inherent risk.*

*This creates a significant burden for any possible financial customers of the ID verification company in Australia – they would have to sufficiently convince APRA that this operation was a risk they could manage, creating a timely and costly set of regulatory hurdles for the customer to undertake. As a result, cloud providers servicing Australian financial services firms tend to host financial data on local services.*

*While not a direct barrier to market entry for the UK company, this level of compliance and regulator engagement creates a de facto data localisation requirement for certain firms that operate within the financial services sector trying to enter the Australian market. The impact is particularly large for start-ups and smaller operators who do not have the institutional capacity to set up a local data storage and processing arrangement.*

**"Australia's domestic financial regulatory regime in respect of outsourcing and cloud services provisions can, under certain circumstances, operate as a de facto localisation requirement."**

# Recommendations

**As one of the few countries currently pursuing an expansive trade liberalisation agenda, the UK is in a strong position to set the agenda on digital trade, and financial services in particular. UK trade negotiations offer an opportunity to secure greater assurances for British financial firms reliant on data transfers. And while opportunities to improve the digital trade landscape via CPTPP accession are limited given its rule book is already written (although it will allow the UK to plug gaps in coverage with New Zealand on, for example, source code protection), the UK could negotiate supplementary Digital Economy Agreements with its members, as it has already done with Singapore.**

**However, there is a need for realism. Given the breadth of the available carve-outs and exceptions in existing UK (and other) FTAs, policymakers and regulators need to take a step further in their commitments to digital trade.**

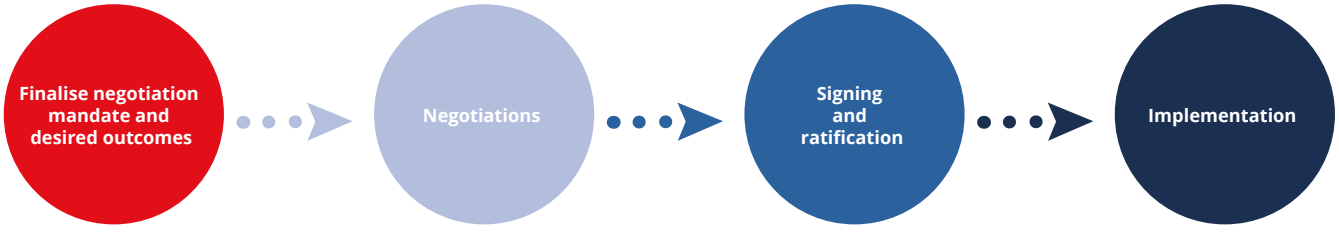
**With that in mind, below are suggestions for how the UK could improve the effectiveness of its digital trade provisions, and their commercial relevance for the UK's financial services sector, given the importance of the sector to the UK economy and economic recovery post-Covid.**

## 1.
## Increased involvement of regulators in defining negotiation terms and objectives

If the digital provisions of FTAs are to work in practice and prevent, for example, financial regulators creating de-facto financial data localisation requirements, the regulators need to understand, agree with, and be invested in making them work in practice. This would require relevant regulators in the UK such as the Prudential Regulatory Authority, the Bank of England and the Financial Conduct Authority, being involved and engaged in the pre-negotiation (red) setting of the mandate, preferred outcomes and objectives, and negotiations themselves. Regulators should recognise that a balkanised world of financial data makes their job much harder and that it's in their interests to ensure that the firms they supervise can provide the data they need for oversight.

Regulator involvement throughout the negotiating process would allow for a greater level of specificity in the negotiation and the direct linkage of trade provisions to existing and proposed regulatory interventions. It would also ensure that they have a vested interested in the full-implementation of digital commitments, and increase their level of comfort with commitments made.

**"Regulator involvement throughout the negotiating process would allow for a greater level of specificity in the negotiation and the direct linkage of trade provisions to existing and proposed regulatory interventions."**



## 2.

## Build regulatory dialogues around specific concrete commitments

Carve-outs and exceptions mean that there is little obligation on financial services regulators to accommodate new FTA commitments, or alter pre-existing approaches, unless they want to do so.

Trade agreements should clearly outline the conditions applicable to financial data, provide clarity on how terms within the agreement should be interpreted by regulators and the parties, and be constructed in a way to limit the scope for de-facto data localisation. The goal should be to positively detail legitimate regulatory requirements and language that prohibits negative and illegitimate policy actions like data localisation, to avoid the potential that countries misuse exceptions.

The UK-New Zealand FTA [**Article 8.63**] sets a precedent here, using constructive language limiting the exceptions on the free flow of financial data and placing a set of obligations on the party to undertake when looking to impose data localisation measures on a financial services supplier. However, for the terms to be meaningful and achieve their intended purpose, it is essential that partner countries and their respective regulators develop a shared understanding of what the various commitments mean in practice.

New and existing FTAs should be supplemented by other trade policy tools to address barriers such as joint regulator-to-regulator memorandums of understanding – similar in nature to the HM Treasury and Monetary Authority of Singapore MoU on financial services regulatory cooperation – with the explicit purpose of ensuring the digital trade provisions are effectively implanted. Doing so would bind the respective regulators to engage with the spirit of the FTAs, and their liberalisation objectives.

This digital MoU could:

- Commit the relevant financial regulators to reach and jointly-publish a shared understanding of what constitutes a legitimate reason to require the onshoring of financial data. This should include agreed understanding on specific definitions and terms of the deal such as what 'consult', 'timely' and 'objective' mean in a precise way, and be accompanied by guidance setting out concrete requirements firms can take to ensure they do not fall foul of any localisation rules, for example the processes they should have in place to ensure information is readily available to both regulators for the purpose of financial regulation and supervision.
- Require the relevant regulators to identify, list and justify all pre-existing regulatory measures that could result in either the UK or its partner country breaching the FTA's digital trade commitments. This should include regulators assessing all credible alternative solutions to localisation to achieve their objectives.
- Impose a 3/6-month deadline on the relevant regulators reaching agreement on the above.
- Introduce a transition/consultation period when making policy changes which would affect digital trade or data localisation rules.

**"New and existing FTAs should be supplemented by other trade policy tools to address barriers such as joint regulator-to-regulator memorandums of understanding."**

## 3.
## Trigger mechanism for escalation

Countries are, understandably, never going to give up their right to regulate and intervene, in the event of a security or financial crisis. However, firms should be able to raise a formal query when a country or regulator breaches the terms of a FTA. Regulators should also be required to formally justify new restrictions, and the use of an FTA's carve-outs or exceptions.

Existing and future UK FTAs should expand on current consultation provisions for financial services (**see Box 8** for an example) –which only allow governments to raise concerns – by including a consultation mechanism for relevant stakeholders. They should set out a process for good faith engagement and structured escalation, allowing stakeholders to flag and challenge both existing and emerging concerns.

**BOX 8:**
**UK-NEW ZEALAND FTA, ARTICLE 11.17 CONSULTATION**

*A Party may request consultations with the other Party regarding any matter arising under the Agreement that affects financial services. The other Party shall give sympathetic consideration to the request. The consulting Parties shall report the results of their consultations to the Working Group.*

*Each Party shall ensure that when there are consultations pursuant to paragraph 1, its delegation includes officials with the relevant expertise in the area covered by this Chapter. For the United Kingdom, this includes officials of HM Treasury or its successor. For New Zealand, this includes officials from the Ministry of Foreign Affairs and Trade, in coordination with financial services regulators.*

*For greater certainty nothing in this Article shall be construed to require a Party to derogate for its law regarding sharing of information between regulatory authorities, or the requirements of an agreement or arrangement between financial authorities of the Parties, or to require a regulatory authority to take any action that would interfere with specific regulatory, supervisory, administrative, or enforcement matters.*



**"Existing and future UK FTAs should expand on current consultation provisions for financial services."**

## 4.
## Prioritise data adequacy

Facilitating the international transfer of personal data is particularly tricky and has second-order implications for the transfer of financial data. As per the recent International Regulatory Strategy Group report 'The future of international data transfers'[31], the ideal solution would be a global set of mutually acceptable principles that would underpin an international outcomes-based approach to privacy and the free flow of personal data. Failing that, plurilateral agreements based on overarching codes of conduct and certifications would be a step in the right direction.

However, in the immediate term, the UK should prioritise its data adequacy agreements, and their application both to existing and future FTA partners that have equivalent levels of data protection. These would allow for personal data to flow more freely between the UK and covered third parties, and facilitate the transfer of financial data with associated economic benefits (**see Case Study 3**). In order to achieve this, the UK's adequacy team within the Department for Digital, Culture, Media and Sport (DCMS), the trade team within HM Treasury, and the digital trade team within the Department for International Trade (DIT) need to work together and create a practical strategy on how to attain these data agreements and ensure the free flow of personal data as a team. When growing its number of adequacy agreements, the UK will need to be careful not to jeopardise its own EU adequacy status – and proactively engage with the European Commission and others to alleviate any concerns about so-called data laundering.

**CASE STUDY 3:**
## JAPAN

*The UK-Japan Comprehensive Economic Partnership Agreement (CEPA) was the UK's first post-Brexit new FTA. UK promotional material states that the deal goes beyond the EU's deal with Japan as it includes specific bans on unjustified data localisation and limits restrictions on the free flow of data between markets.*

*However, there is no evidence of pre-existing restrictions on data flows between Japan and the UK. The free flow of personal data is already ensured under Japan's data adequacy agreement with the UK, rolled over from the EU's 2019 decision, whereby personal data is able to transfer freely between the two markets for processing and storage. CEPA provides no additional market access beyond what was already in place*

*In the absence of an adequacy arrangement, there would be greater onus on companies to ensure the protection of personal financial data sent out of Japan. UK financial services operating in Japan, but transferring personal data back to the UK, would need to take steps to assess each transfer individually to determine if they can safely and legally send data. Companies would need to obtain consent from the individual data subjects or ensure that mechanisms were in place to provide adequate safeguards when exporting personal data, such as Standard Contractual Clauses or Binding Corporate Rules. These create increased compliance obligations for companies and can be costly and time consuming.*

*Whilst the adequacy agreement does allow for personal data to be transferred freely between the UK and Japan, there is a lack of transparency and understanding about how this operates in practice. UK firms are sometimes reluctant to rely on the agreement as regulatory guidelines are provided in Japanese, with considerable uncertainty about the rules regarding health data. Confusion about how adequacy operates in practice can pose a barrier to market entry, particularly for smaller sized enterprises.*

# Conclusion

The UK wants to be a global leader in digital trade; it has demonstrated a willingness to pursue progressive digital trade deals, remove digital barriers to trade and facilitate the free flow of data and ideas. The provisions in the UK-Singapore Digital Economy Agreement in particular can rightfully be described as cutting edge.

Yet the question of whether digital provisions in new UK FTAs are of commercial use to financial services firms remains an open one. Regulators and governments regularly use existing carve outs and exceptions under the guise of privacy, prudential and national security concerns to restrict market access for foreign services firms, in breach of FTA commitments. If regulators continue to be treated as peripheral to the FTA negotiation process, and have no stake in their successful implementation, firms will remain unable to rely on the digital trade commitments agreed to in FTAs, depriving them of further growth and innovation opportunities and subsequent benefits to the UK economy.

The UK now has the opportunity to build on existing agreements, and further integrate trade and regulatory policy making. The suggestions made in this report would be a significant step forward in ensuring the UK free trade agenda delivers tangible commercial benefits for the financial services sector.

# Annex

**Relevant digital provisions for financial services – text and exceptions.**

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Customs Duties** | The Parties shall not impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.<br><br>Does not preclude a Party from imposing internal taxes, fees or other charges on electronic transmissions, provided that those taxes, fees or charges are imposed in a manner consistent with this Agreement. | Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.<br><br>Does not preclude a Party from imposing internal taxes, fees or other charges on electronic transmissions, including content transmitted electronically, provided that those taxes, fees or charges are imposed in a manner consistent with this Agreement. | Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.<br><br>Shall not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions, including content transmitted electronically, provided that those taxes, fees, or charges are imposed in a manner consistent with this Agreement.<br><br>The Parties shall cooperate in relevant international fora to promote the adoption of commitments by non-parties not to impose customs duties on electronic transmissions. | Neither Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of a Party and a person of the other Party.<br><br>Shall not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions, including content transmitted electronically, provided that such taxes, fees, or charges are imposed in a manner consistent with this Agreement. |
| **Domestic regulation** | Each Party shall ensure that all its measures of general application affecting electronic commerce, including measures related to its collection of information, are administered in a reasonable, objective and impartial manner. | Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 ... or the United Nations Convention on the Use of Electronic Communications in International Contracts.<br><br>Each Party shall endeavour to: (a) avoid any unnecessary regulatory burden on electronic transactions; and (b) facilitate input by interested persons in the development of its legal framework for electronic transactions.<br><br>The Parties recognise the importance of developing mechanisms to facilitate the use of electronic transferable records. To this end, in developing such mechanisms, the Parties shall endeavour to take into account, as appropriate, relevant model legislative texts developed and adopted by international bodies, such as the UNCITRAL Model Law on Electronic Transferable Records 2017. | Paragraph 1 & 2 same as UK-Australia<br><br>The Parties recognise the importance of facilitating the use of electronic transferable records. When developing measures relating to electronic transferable records, each Party shall take into account the UNCITRAL Model Law on Electronic Transferable Records. | Paragraph 1 & 2 same as UK-Australia<br><br>The Parties recognise the importance of facilitating the use of electronic transferable records. To this end, each Party shall endeavour to establish a legal framework governing electronic transferable records consistent with the UNCITRAL Model Law on Electronic Transferable Records 2017. |
| **Electronic Contracts** | A Party shall not adopt or maintain measures regulating electronic transactions that: (a) deny the legal effect, validity or enforceability of a contract, solely on the grounds that it is concluded by electronic means; or (b) otherwise create obstacles to the use of contracts concluded by electronic means. | Each Party shall ensure that: its legal framework allows for contracts to be concluded by electronic means; and<br><br>its law neither creates obstacles for the use of electronic contracts nor results in electronic contracts being deprived of legal effect, enforceability, or validity, solely on the ground that the contract has been made by electronic means.<br><br>The Parties recognise the importance of transparency for minimising barriers to the use of electronic contracts in digital trade. To that end, each Party shall: (a) promptly publish the circumstances referred to [above] on a single official website hosted by the central level of government; and (b) review these circumstances with a view to reducing them over time. | A Party shall not adopt or maintain measures that: deprive an electronic contract of legal effect, enforceability, or validity, solely on the ground that the contract has been made by electronic means; or otherwise create obstacles for the use of electronic contracts.<br><br>Recognising the importance of increasing the use of electronic contracts, the Parties should review and reduce the circumstances referred to [above]. | Neither Party shall deny the legal effect, legal validity or enforceability of an electronic contract, solely on the basis that the contract has been concluded by electronic means.<br><br>Recognising the importance of transparency for minimising barriers to digital trade, each Party shall maintain on a publicly accessible website a list of the circumstances referred to [electronic contracts].<br><br>With the aim of increasing the use of electronic contracts, each Party shall review its list... on an ongoing basis. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **E-Signatures / Electronic Authentication** | A Party shall not deny the legal effect or validity of an electronic signature or the authenticating data resulting from electronic authentication, solely on the grounds that it is in electronic form.<br><br>A Party shall not adopt or maintain measures regulating electronic authentication and electronic signature that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods for their transaction; or (b) prevent parties to an electronic transaction from being able to prove to judicial or administrative authorities that the use of electronic authentication or an electronic signature in that transaction complies with the applicable legal requirements.<br><br>Each Party may require that, for a particular category of transactions, the method of electronic authentication or electronic signature meets certain performance standards which shall be objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned or is certified by an authority accredited in accordance with its laws and regulations.<br><br>The Parties shall encourage the use of interoperable electronic authentication and electronic signatures. | Neither Party shall deny the legal validity or effect or admissibility of an electronic document or signature solely on the basis that the signature is in electronic form.<br><br>Neither Party shall adopt or maintain measures that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods for that transaction; or<br><br>(b) prevent parties to an electronic transaction from being able to prove to judicial or administrative authorities that the use of electronic authentication in that transaction complies with the applicable legal requirements<br><br>A Party may require that for a particular category of transactions, the method of electronic authentication is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent, and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.<br><br>The Parties shall encourage the use and mutual recognition of interoperable electronic authentication.<br><br>A Party shall apply [the above] to other electronic processes or means of facilitating or enabling electronic transactions, such as electronic seals, electronic time stamps, electronic registered delivery services, or electronic trust services. | Neither Party shall deny the legal effect or admissibility as evidence in legal proceedings of an electronic document, an electronic signature, an electronic seal, or the authenticating data resulting from electronic authentication, solely on the ground that it is in electronic form.<br><br>Paras 2 & 3 same as UK-Australia.<br><br>Parties shall encourage the use of interoperable electronic authentication and recognise the benefits of working towards mutual recognition of electronic authentication. To this end, the Parties shall endeavour to share information, where appropriate, on matters related to e-authentication.<br><br>A Party shall apply [the above] to electronic processes or means of facilitating or enabling electronic transactions, such as electronic time stamps and electronic registered delivery services. | A Party shall not deny the legal validity or legal effect of an electronic signature solely on the basis that the signature is in electronic form<br><br>Para 2 same as UK-Australia.<br><br>A Party may require that for a particular category of transactions, the method of electronic authentication is certified by an authority accredited in accordance with its law or meets certain performance standards which shall be objective, transparent, and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.<br><br>The Parties shall encourage the use of interoperable electronic authentication, and recognise the benefits of working towards mutual recognition of electronic authentication. To this end, the Parties shall endeavour to share information, where appropriate, on matters related to e-authentication<br><br>Para 5 same as UK-New Zealand. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Electronic Invoicing** | N/A | The Parties recognise the importance of electronic invoicing to increase the efficiency, accuracy, and reliability of commercial transactions. Each Party also recognises the benefits of ensuring that the systems used for electronic invoicing within its territory are interoperable with the systems used for electronic invoicing in the other Party's territory.<br><br>Each Party shall endeavour to ensure that the implementation of measures related to electronic invoicing in its territory supports cross-border interoperability between the Parties' electronic invoicing frameworks. To this end, the Parties shall take into account international frameworks when developing measures related to electronic invoicing.<br><br>The Parties recognise the economic importance of promoting the global adoption of interoperable electronic invoicing systems. To this end, the Parties shall endeavour to share best practices and collaborate on promoting the adoption of interoperable systems for electronic invoicing. | The Parties recognise the importance of e-invoicing to increase the efficiency, accuracy, and reliability of commercial transactions. Each Party also recognises the benefits of ensuring interoperability of e-invoicing systems to support digital trade and that these systems can be used for business-to-business and business-to-consumer digital transactions.<br><br>Each Party shall ensure that the implementation of measures related to e-invoicing in its jurisdiction is designed to support cross-border interoperability. When developing measures related to e-invoicing, each Party shall take into account international frameworks, guidelines, or recommendations, where these exist.<br><br>The Parties shall share best practices pertaining to e-invoicing. | Para 1 same as UK-Australia<br><br>Each Party shall ensure that the implementation of measures related to electronic invoicing in its territory supports cross-border interoperability between the Parties' electronic invoicing frameworks. To this end, each Party shall take into account international frameworks when developing measures related to electronic invoicing, such as Peppol.<br><br>The Parties recognise the economic importance of promoting the global adoption of interoperable electronic invoicing systems. To this end, the Parties shall share best practices and collaborate, where appropriate, on promoting the adoption of interoperable systems for electronic invoicing.<br><br>The Parties recognise the benefits of promoting, encouraging, supporting or facilitating the adoption of electronic invoicing by juridical persons. To this end, the Parties shall endeavour to promote the existence of policies, infrastructure or processes that support electronic invoicing. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Paperless Trading** | N/A | Each Party shall endeavour to: (a) make trade administration documents available to the public in electronic form; and (b) accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document.<br><br>The Parties shall cooperate bilaterally and in international fora, where appropriate, to promote acceptance of electronic versions of trade administration documents and on other matters related to paperless trading.<br><br>In developing initiatives concerning the use of paperless trading, the Parties shall endeavour to take into account the principles and guidelines of relevant international bodies. | Each party shall make trade administration documents that it issues or controls available to the public in electronic form.<br><br>Each Party shall endeavour to accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document.<br><br>The Parties shall, where appropriate, cooperate bilaterally and in international fora on matters related to paperless trading, such as enhancing the standardisation and acceptance of electronic trade administration documents.<br><br>In developing initiatives concerning the use of paperless trading, each Party shall take into account the principles and guidelines agreed by relevant international bodies. | The Parties recognise the importance of digital connectivity in enabling trade. To this end, the Parties aim to facilitate cross-border supply chain digitalisation with a focus on interoperability.Each Party shall make trade administration documents available to the public in electronic form and in English.<br><br>Each Party shall accept completed electronic versions of trade administration documents as the legal equivalent of paper documents, except where that Party is: (a) subject to a domestic or international legal requirement to the contrary; or<br><br>(b) doing so would reduce the effectiveness of the trade administration process.<br><br>The Parties shall, where appropriate, cooperate bilaterally and in international fora on matters related to paperless trading, including by promoting the acceptance of electronic versions of trade administration documents and supporting documents.<br><br>In developing initiatives concerning the use of paperless trading, each Party shall endeavour to take into account the principles and guidelines of relevant international bodies. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Online Consumer Protection** | The Parties recognise the importance of adopting and maintaining transparent and effective consumer protection measures applicable to electronic commerce as well as measures conducive to the development of consumer confidence in electronic commerce.<br><br>Each Party shall adopt or maintain consumer protection laws and regulations to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.<br><br>The Parties recognise the importance of and shall promote cooperation between their respective competent authorities in charge of consumer protection on activities related to electronic commerce in order to enhance consumer protection and welfare. To this end, the Parties affirm that cooperation under [online consumer protection article] includes cooperation with respect to online commercial activities. | The Parties recognise the importance of transparent and effective measures that enhance consumer confidence and trust in digital trade.<br><br>Each Party shall maintain consumer protection laws and regulations that proscribe: (a) misleading, deceptive, and fraudulent commercial practices; and (b) unconscionable conduct or unfair commercial practices, that cause harm, or potential harm, to consumers engaged in digital trade.<br><br>The Parties recognise the importance of, and where appropriate shall promote, cooperation between their respective national consumer protection agencies or other relevant bodies on activities aimed at online consumer protection.<br><br>The Parties further recognise the importance of improving awareness of and providing access to consumer redress mechanisms to protect consumers engaged in digital trade, including for consumers of a Party transacting with suppliers of the other Party.<br><br>The Parties recognise the benefits of dispute resolution mechanisms in facilitating the resolution of disputes regarding electronic commerce transactions, including alternative dispute resolution mechanisms. | Each Party shall provide consumers engaged in online commercial activities with a level of protection not less than that provided under its law to consumers engaged in other forms of commerce. | The Parties recognise the importance of adopting and maintaining transparent and effective measures that contribute to consumer trust in digital trade.<br><br>To this end, each Party shall adopt or maintain measures that protect consumers engaged in digital trade, including laws and regulations that proscribe misleading, deceptive, fraudulent, and unfair commercial practices that cause harm or potential harm to consumers.<br><br>The Parties recognise the importance of, and where appropriate, shall promote cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to digital trade in order to enhance consumer welfare.<br><br>The Parties further recognise the importance of improving awareness of, and providing access to, consumer redress mechanisms to protect consumers engaged in digital trade, including for consumers of a Party transacting with suppliers of the other Party.<br><br>The Parties shall endeavour to explore the benefits of mechanisms, including alternative dispute resolution, to facilitate the resolution of disputes concerning digital trade. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Digital Identities** | N/A | Recognising that cooperation between the Parties on digital identities will increase regional and global connectivity, and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall pursue the development of mechanisms to promote compatibility between their respective digital identity regimes.<br><br>To this end, the Parties shall endeavour to facilitate initiatives to promote such compatibility, which may include: (a) developing appropriate frameworks and common standards to foster technical interoperability between each Party's implementation of digital identities; (b) supporting the development of international frameworks on digital identity regimes; (c) implementing use cases for the mutual recognition of digital identities; and (d) exchanging knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation, security standards, and the promotion of the use of digital identities. | The Parties recognise that: (a) the cooperation of the Parties on digital identities will increase regional and global connectivity; and (b) each Party may have different implementations of, and legal approaches to, digital identities.<br><br>The Parties shall strengthen cooperation and facilitate initiatives to promote compatibility and interoperability between their respective regimes for digital identities, including exploring: (a) the development and maintenance of appropriate frameworks to increase technical and service interoperability between each Party's implementation of digital identities; (b) supporting the development of international frameworks on digital identity regimes; (c) identifying use cases for the mutual recognition of digital identities; and (d) the exchange of knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, promotion, and user adoption.<br><br>For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with [above] to achieve a legitimate public policy objective. | Recognising that cooperation between the Parties on digital identities will increase regional and global connectivity, and recognising that each Party may take different legal and technical approaches to digital identities, the Parties shall pursue the development of mechanisms to promote compatibility and interoperability between their respective digital identity regimes.<br><br>To this end, the Parties shall endeavour to facilitate initiatives to promote such compatibility and interoperability, which may include: (a) developing appropriate frameworks and common standards to foster technical interoperability between each Party's implementation of digital identities; (b) developing comparable protection of digital identities under each Party's respective legal frameworks, or the recognition of their legal effects, whether accorded autonomously or by agreement; (c) supporting the development of international frameworks on digital identity regimes; (d) identifying and implementing use cases for the mutual recognition of digital identities; and (e) exchanging knowledge and expertise on best practices relating to digital identity policies and regulations, technical implementation and security standards, and the promotion of the use of digital identities. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Unsolicited Commercial Electronic Communications** | Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or (b) require the prior consent, as specified according to its laws and regulations, of recipients to receive commercial electronic messages.<br><br>Each Party shall ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable recipients to request cessation free of charge and at any time.<br><br>Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to [measures above]. | Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require a supplier of unsolicited commercial electronic messages to facilitate the ability of a recipient to prevent ongoing reception of those messages; (b) require the consent, as specified according to its laws and regulations, of recipients to receive commercial electronic messages; or (c) otherwise provide for the minimisation of unsolicited commercial electronic messages.<br><br>Each Party shall ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable recipients to request cessation free of charge and at any time.<br><br>Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to [measures above].<br><br>The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages. | Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or (b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages, and otherwise provide for the minimisation of unsolicited commercial electronic messages.<br><br>Each Party shall ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable recipients to request cessation free of charge and at any time.<br><br>Each Party shall provide access to either redress or recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to [measures above].<br><br>The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages. | Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or (b) require the consent, as specified in the laws and regulations of that Party, of recipients to receive commercial electronic messages.<br><br>Each Party shall ensure that unsolicited commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are made, and to the extent provided for in a Party's laws and regulations, contain the necessary information to enable end-users to request cessation free of charge and at any time.<br><br>Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained in accordance with [measures above].<br><br>The Parties shall endeavour to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Commercial Information and Communication Tech Products that use cryptography** | A Party shall not require a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import or use of the commercial ICT product, to: (a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, to that Party or a person in the territory of that Party; (b) partner or otherwise cooperate with a person in the territory of that Party in the development, manufacture, sale, distribution, import or use of the commercial ICT product; or (c) use or integrate a particular cryptographic algorithm or cipher.<br><br>This Article shall not preclude a regulatory body or judicial authority of a Party from requiring a manufacturer or supplier of a commercial ICT product that uses cryptography: (a) to preserve and make available any information to which subparagraph 1(a) applies for an investigation, inspection, examination, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure; or (b) to transfer or provide access to any information to which subparagraph 1(a) applies for the purpose of imposing or enforcing a remedy granted in accordance with that Party's competition law following an investigation, inspection, examination, enforcement action or judicial proceedings.<br><br>This Article applies to commercial ICT products that use cryptography. This Article does not apply to: (a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures; (b) the regulation of financial instruments; (c) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks; (d) measures by a Party adopted or maintained pursuant to supervisory, investigatory or examination authority relating to financial service suppliers or financial markets; or (e) the manufacture, sale, distribution, import or use of a commercial ICT product that uses cryptography by or for a Party. | Neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import, or use of the ICT product, to:<br><br>(a) transfer or provide access to a particular technology, production process, or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product to the Party or a person in the Party's territory; (b) partner or otherwise cooperate with a person in the Party's territory in the development, manufacture, sale, distribution, import, or use of the ICT product; or<br><br>(c) use or integrate a particular cipher or cryptographic algorithm.<br><br>This Article does not apply to: (a) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks; (b) measures by a Party adopted or maintained pursuant to supervisory, investigatory, or examination authority relating to financial service suppliers or financial markets; or (c) the manufacture, sale, distribution, import, or use of the commercial ICT product by or for a Party.<br><br>For greater certainty, this Article shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, access to encrypted and unencrypted communications. | Neither Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import, or use of that commercial ICT product, to: (a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail, to that Party or a person in the territory of that Party;<br><br>(b) partner or otherwise cooperate with a person in the territory of that Party in the development, manufacture, sale, distribution, import, or use of the commercial ICT product; or<br><br>(c) use or integrate a particular cipher or cryptographic algorithm.<br><br>This Article shall apply to commercial ICT products that use cryptography. This Article shall not apply to: (a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures; (b) the regulation of financial instruments; (c) a requirement that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks; (d) measures by a Party adopted or maintained pursuant to supervisory, investigatory, or examination authority relating to financial service suppliers or financial markets; (e) the manufacture, sale, distribution, import, or use of a commercial ICT product by or for a Party; or (f) a commercial ICT product other than a good. | This Article applies to commercial ICT products that use cryptography. This Article does not apply to: (a) a Party's law enforcement authorities requiring service suppliers using encryption to provide access to encrypted and unencrypted communications pursuant to that Party's legal procedures; (b) the regulation of financial instruments; (c) measures that a Party adopts or maintains relating to access to networks, including user devices, that are owned or controlled by that Party, including those of central banks; (d) measures that a Party adopts or maintains pursuant to supervisory, investigatory or examination authority relating to financial service suppliers or financial markets; or (e) the manufacture, sale, distribution, import or use of a commercial ICT product by or for a Party.<br><br>Neither Party shall require a manufacturer or supplier of a commercial ICT product that uses cryptography, as a condition of the manufacture, sale, distribution, import or use of the commercial ICT product, to: (a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, to that Party or a person in the territory of that Party; (b) partner or otherwise cooperate with a person in the territory of that Party in the development, manufacture, sale, distribution, import or use of the product; or (c) use or integrate a particular cryptographic algorithm.<br><br>This Article shall not preclude a regulatory body or judicial authority of a Party from requiring a manufacturer or supplier of a commercial ICT product that uses cryptography to: (a) preserve and make available any information to which paragraph 2(a) applies for an investigation, inspection, examination, enforcement action or a judicial proceeding, subject to safeguards against unauthorised disclosure; or (b) transfer or provide access to any information to which paragraph 2(a) applies for the purpose of imposing or enforcing a remedy granted in accordance with that Party's competition law following an investigation, inspection, examination, enforcement action or a judicial proceeding.<br><br>For greater certainty, this Article does not affect the rights and obligations of a Party under [Source Code Article]. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Protection of personal information** | The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.<br><br>To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.<br><br>Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.<br><br>Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements.<br><br>Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. | The Parties recognise the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.<br><br>To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies, including collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability.<br><br>Each Party shall adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.<br><br>Each Party shall publish information on the personal information protections it provides to users of digital trade, including how: (a) a natural person can pursue a remedy; and (b) an enterprise can comply with any legal requirements.<br><br>Each Party shall encourage enterprises in its territory to publish, including on the Internet, their policies and procedures related to protection of personal information.<br><br>Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. | The Parties emphasise the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.<br><br>Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. . In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies.<br><br>The Parties recognise that the principles underpinning a robust personal information protection framework include: (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) openness; (g) individual participation; and (h) accountability.<br><br>Each Party shall adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.<br><br>Each Party shall publish information on the personal information protections it provides to users of digital trade, including how: (a) an individual can pursue a remedy; and (b) an enterprise can comply with any legal requirements.<br><br>Each Party shall pursue the development of mechanisms to promote compatibility and interoperability between these different regimes for protecting personal information. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall exchange information on any mechanisms applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them. | The Parties recognise the economic and social benefits of protecting the personal information of natural persons who are involved in digital trade, including electronic transactions, and the contribution that this makes to enhancing consumer confidence in the digital economy and the development of trade.<br><br>To this end, each Party shall adopt or maintain a legal framework that provides for the protection of personal information of natural persons who are involved in digital trade, including electronic transactions. In the development of its legal framework for the protection of personal information, each Party shall take into account the principles and guidelines of relevant international bodies.<br><br>The Parties agree that the key principles for its legal framework, which take into account the principles of relevant international bodies, shall include: limitation on collection; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability.<br><br>Each Party shall adopt non-discriminatory practices in protecting natural persons who are involved in digital trade, including electronic transactions, from personal information protection violations occurring within its territory.<br><br>Each Party shall publish information on the personal information protections it provides to natural persons who are involved in digital trade, including electronic transactions, including how: (a) a natural person can pursue a remedy; and (b) a juridical person can comply with any legal requirements.<br><br>Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development and adoption of mechanisms to promote compatibility and interoperability between these different regimes. These mechanisms may include mutual arrangements, or broader international frameworks. The Parties recognise that in accordance with their respective laws and regulations, there are existing mechanisms, including contractual provisions, for the transfer of personal information between their respective territories.<br><br>The Parties shall endeavour to exchange information on how the mechanisms in paragraph 6 are applied in their respective territory and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Data Flows** | A Party shall not prohibit or restrict the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.<br><br>Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with [above] to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.<br><br>This Article does not apply to: (a) government procurement; or (b) information held or processed by or on behalf of a Party, or measures by a Party related to that information, including measures related to its collection. | The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.<br><br>Neither Party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person.<br><br>Public Policy Exception same as UK-Japan | First paragraph same as UK-Australia.<br><br>Each Party shall allow the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of the business of a covered person.<br><br>Public Policy Exception same as UK-Japan. | Same as UK-Australia |
| **Data Localisation (Location of computing facilities)** | A Party shall not require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.<br><br>Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with [above] that are necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.<br><br>This Article does not apply to: (a) government procurement; or (b) information held or processed by or on behalf of a Party, or measures by a Party related to that information, including measures related to its collection. | The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.<br><br>Neither Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.<br><br>Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with [above] to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective. | Same as UK-Australia | Same as UK-Australia |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Financial data flows (Financial data and information)** | A Party shall not restrict a financial service supplier of the other Party from transferring information, including transfers of data into and out of the former Party's territory by electronic or other means, where such transfers are relevant for the conduct of the ordinary business of the financial service supplier. | The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means and the use of financial service computing facilities, including requirements that seek to ensure the security and confidentiality of communications.<br><br>Neither Party shall prohibit or restrict a financial service supplier of the other Party from transferring, including by electronic means, information including personal information, where those transfers are necessary for the conduct of the ordinary business of the financial service supplier.<br><br>Nothing shall restrict the right of a Party to adopt or maintain measures inconsistent with [the above] to achieve a legitimate public policy objective such as the protection of personal information, personal privacy, and the confidentiality of individual records and accounts, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information or on the use or location of computing facilities greater than are required to achieve the objective.<br><br>This Article does not apply to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection.<br><br>This Article does not apply to credit information, or related personal information, of a natural person. | Neither Party shall restrict a financial service supplier of the other Party from transferring information, including transfers of data by electronic means, where such transfers are necessary for the conduct of the ordinary business of the financial service supplier.<br><br>Subject to [below], it is prohibited for a Party to require, as a condition for conducting business in the Party's territory, a financial service supplier of the other Party to use, store, or process information in the Party's territory. This prohibition also applies to circumstances in which a financial service supplier of the other Party uses the services of an external business for such use, storage, or processing of information.<br><br>Each Party has the right to require that information of a financial service supplier of the other Party is used, stored, or processed in its territory, where it is not able to ensure access to information required for the purposes of financial regulation and supervision, provided that the following conditions are met: (a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and (b) the Party or its regulatory authorities consult the other Party or its regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use, store, or process information in its territory.<br><br>Nothing in this Article shall restrict the right of a Party to adopt or maintain measures inconsistent with [the above] to achieve a legitimate public policy objective, such as the protection of personal data, personal privacy, and the confidentiality of individual records and accounts, provided that such measures: (a) are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) do not impose restrictions on transfers of information greater than are required to achieve the objective.<br><br>Exception – doesn't apply to NZ's overseas investment approval framework. | Neither Party shall, subject to appropriate safeguards on privacy and confidentiality, prohibit or restrict a financial service supplier of the other Party from transferring information in electronic or other form, into and out of its territory, where such transfer is required in the ordinary course of business of such financial service supplier. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Financial data localisation (Location of Financial Service Computing Facilities for Covered Financial Service Suppliers)** | Subject to [below], a Party shall not require, as a condition for conducting business in its territory, a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.<br><br>A Party has the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure access to information that is appropriate for the purposes of effective financial regulation and supervision, provided that the following conditions are met: (a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and (b) the Party or its financial regulatory authorities consults the other Party or its financial regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.<br><br>Nothing [above] shall be construed to grant a Party access to information or to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, in a manner beyond what is appropriate for the purposes of effective financial regulation and supervision.<br><br>Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as that right is not used to circumvent [the above].<br><br>For greater certainty, "appropriate" access may include sufficient and timely access that is provided without undue delay for the purposes of regulation and supervision. | The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means and the use of financial service computing facilities, including requirements that seek to ensure the security and confidentiality of communications.<br><br>Subject to [below], it is prohibited for a Party to require, as a condition for conducting business in the Party's territory, a financial service supplier of the other Party to use or locate financial service computing facilities, in the former Party's territory.<br><br>*(For greater certainty, this prohibition also applies to circumstances in which a financial service supplier of the other Party uses the services of an external business for such use, storage or processing of information)<br><br>Each Party has the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure appropriate access to information required for the purposes of financial regulation and supervision, provided that the following conditions are met: (a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and (b) the Party or its regulatory authorities inform the other Party or its regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.<br><br>Nothing shall restrict the right of a Party to adopt or maintain measures inconsistent with [above] to achieve a legitimate public policy objective such as the protection of personal information, personal privacy, and the confidentiality of individual records and accounts, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information or on the use or location of computing facilities greater than are required to achieve the objective.<br><br>This Article does not apply to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection.<br><br>This Article does not apply to credit information, or related personal information, of a natural person. | Neither Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.<br><br>Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:<br><br>(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and<br><br>(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective | Subject to [below] and to appropriate safeguards on privacy and confidentiality, it is prohibited for either Party to require, as a condition for conducting business in the Party's territory, a financial service supplier of the other Party to use or locate financial service computing facilities, in the former Party's territory.<br><br>Each Party shall have the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure appropriate access to information required for the purposes of financial regulation and supervision, provided that the following conditions are met: (a) to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and (b) the Party or its regulatory authorities consult the other Party or its regulatory authorities before imposing any requirements on a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory.<br><br>Each Party shall adopt or maintain appropriate safeguards to protect privacy and personal data, including individual records and accounts, as long as these safeguards are not used to circumvent the provisions of this Agreement. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Cooperation on electronic commerce** | The Parties shall, where appropriate, cooperate and participate actively in multilateral fora to promote the development of electronic commerce.<br><br>The Parties agree to maintain a dialogue on regulatory matters relating to electronic commerce with a view to sharing information and experience, as appropriate, including on related laws, regulations and their implementation, and best practices with respect to electronic commerce, in relation to, inter alia: (a) consumer protection; (b) personal information protection; (c) cybersecurity; (d) combatting unsolicited commercial electronic messages; (e) electronic trust services; (f) the treatment of digital products; (g) the recognition of certificates of electronic signatures issued to the public; (h) challenges for small and medium-sized enterprises in the use of electronic commerce; (i) emerging technology, including artificial intelligence and the Internet of Things; (j) the facilitation of cross-border certification services; (k) intellectual property; and (l) electronic government. | Recognising the global nature of digital trade, the Parties shall endeavour to: (a) work together to address challenges for SMEs in the use of digital trade; (b) exchange information and share experiences and best practices on laws, regulations, policies, enforcement, and compliance regarding digital trade, including: (i) personal information protection; (ii) online consumer protection; (iii) unsolicited commercial electronic messages; (iv) cybersecurity; (v) electronic authentication and electronic trust services; (vi) digital government; and (vii) electronic contracts; (c) exchange information and share views on consumer access to products and services offered online between the Parties; (d) participate actively in multilateral fora, including the WTO, to promote the development of international frameworks for digital trade, including in relation to the development and adoption of relevant international standards; (e) work together in areas of mutual interest relating to the development and application of standards and conformity assessment procedures with a view to facilitating digital trade; (f) encourage development by the private sector of methods of self-regulation that foster digital trade, including codes of conduct, model contracts, guidelines, and compliance mechanisms; (g) collaborate to improve opportunities for each Party's RegTech enterprises, including through their respective trade promotion agencies and regulators, and in relevant international fora; and (h) facilitate participation by women in digital trade. | The Parties shall, where appropriate, cooperate and participate actively in international fora, including the WTO, to promote the development of international frameworks for digital trade.<br><br>In addition to areas of cooperation between the Parties identified in other parts of this Chapter, the Parties shall exchange information on and share experiences and best practices on regulatory matters relating to digital trade.<br><br>The Parties shall endeavour to cooperate to promote and facilitate collaboration between governmental entities, enterprises, and other nongovernmental entities on digital technologies and services, including digital innovation and emerging technologies, in relation to opportunities in trade, investment, and research and development, including in the areas of pandemic preparedness, clean technology, and low emissions technology. | The Parties shall, as appropriate, cooperate and participate actively in international fora, including the WTO, to promote the development of international frameworks for digital trade.<br><br>The Parties shall endeavour to: (a) exchange information and share experiences and best practices on regulatory matters relating to the digital economy, including: (i) personal information protection; (ii) data governance; (iii) cross-border data flows; (iv) online consumer protection, including means for consumer redress and building consumer confidence; (v) unsolicited commercial electronic messages; (vi) electronic contracts; (vii) electronic trust and electronic authentication services; (viii) digital identities; (ix) digital trade facilitation; (x) AI and other emerging technology; and (xi) digital government; (b) encourage industry, as appropriate, to develop methods of self-regulation that foster the digital economy, including codes of conduct, model contracts, guidelines and enforcement mechanisms; and (c) exchange information and share best practices on simplified customs procedures applied to expedited shipments. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Cybersecurity** | The Parties agree to maintain a dialogue on regulatory matters relating to electronic commerce with a view to sharing information and experience, as appropriate, including on related laws, regulations and their implementation, and best practices with respect to electronic commerce, in relation to, inter alia: .. cybersecurity. | The Parties recognise that threats to cybersecurity undermine confidence in digital trade. The Parties further recognise the importance of: (a) workforce development in the area of cybersecurity, including possible initiatives relating to mutual recognition of qualifications, diversity, and equality; and (b) enhancing the cybersecurity capability of businesses, including SMEs, and enabling greater cybersecurity resilience within industry.<br><br>The Parties shall endeavour to: (a) build the capabilities of their respective national entities responsible for cybersecurity incident response, taking into account the evolving nature of cybersecurity threats; (b) strengthen existing collaboration mechanisms for cooperating to anticipate, identify, and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents; and (c) maintain a dialogue on matters related to cybersecurity, including for the sharing of information and experiences for awareness and best practices.<br><br>Given the evolving nature of cybersecurity threats, the Parties recognise that risk-based approaches may be more effective than prescriptive approaches in addressing those threats. Accordingly, where appropriate, each Party shall endeavour to employ, and shall encourage enterprises within its jurisdiction to use, risk-based approaches that rely on open and transparent cybersecurity standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events. | The Parties recognise the importance of promoting secure digital trade to achieve global prosperity and recognise that threats to cyber security undermine confidence in digital trade.<br><br>The Parties further recognise the importance of: (a) building the capabilities of their respective national entities responsible for cyber security incident response, taking into account the evolving nature of cyber security threats;<br><br>(b) using and strengthening existing collaboration mechanisms for cooperating to anticipate, identify, and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties, and using those mechanisms to swiftly address cyber security incidents;<br><br>(c) workforce development in the area of cyber security, including through possible initiatives relating to mutual recognition of qualifications, and promoting diversity and equality; and<br><br>(d) maintaining a dialogue on matters related to cyber security, including for the sharing of information and experiences for awareness and best practices.<br><br>Given the evolving nature of cyber security threats, the Parties recognise that risk-based approaches may be more effective than prescriptive approaches in addressing those threats including in the context of digital trade. Accordingly, each Party shall encourage enterprises within its jurisdiction to use risk-based approaches that rely on open and transparent industry standards to: (a) manage cyber security risks and to detect, respond to, and recover from cybersecurity events; and (b) otherwise improve the cyber security resilience of these enterprises and their customers. | The Parties have a shared vision to promote secure digital trade to achieve global prosperity and recognise that threats to cyber security undermine confidence in digital trade. Accordingly, the Parties recognise the importance of: (a) building the capabilities of their respective national entities responsible for cyber security incident response, taking into account the evolving nature of cyber security threats; (b) establishing or strengthening existing collaboration mechanisms to cooperate to anticipate, identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cyber security incidents; (c) maintaining a dialogue on matters related to cyber security, including for the sharing of information and experiences for awareness and best practices; (d) establishing mutual recognition of a baseline security standard for consumer Internet of Things devices to raise overall cyber hygiene levels and better secure cyberspace domestically; (e) workforce development in the area of cyber security, including through possible initiatives relating to training and development; and (f) collaborative cyber security research and development as well as innovation projects among academic, research and business entities.<br><br>Given the evolving nature of cyber security threats, the Parties recognise that risk-based approaches may be more effective than prescriptive, compliance-based approaches in addressing those threats. Accordingly, each Party shall encourage juridical persons within its territory to use risk-based approaches that rely on open and transparent industry standards to: (a) manage cyber security risks and to detect, respond to, and recover from cyber security events; and (b) otherwise improve the cyber security resilience of these juridical persons and their customers. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Source Code** | A Party shall not require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.<br><br>This Article shall not preclude a regulatory body or judicial authority of a Party, or a Party with respect to a conformity assessment body, from requiring a person of the other Party: (a) to preserve and make available the source code of software, or an algorithm expressed in that source code, for an investigation, inspection, examination, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure; or (b) to transfer or provide access to the source code of software, or an algorithm expressed in that source code, for the purpose of imposing or enforcing a remedy granted in accordance with that Party's law following an investigation, inspection, examination, enforcement action or judicial proceedings.<br><br>This Article does not apply to: (a) the voluntary transfer of, or granting of access to, source code, or an algorithm expressed in that source code, by a person of the other Party, such as in the context of a freely negotiated contract or government procurement;(b) services supplied or activities performed in the exercise of governmental authority. | Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, as a condition for the import, distribution, sale, or use of that software, or of a product containing that software, in its territory.<br><br>This Article does not preclude a government agency, regulatory body, administrative tribunal, or judicial authority of a Party, or a designated conformity assessment body operating in the Party's territory, from requiring a person of the other Party to preserve and make available the source code of software for an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding, subject to safeguards against unauthorised disclosure.<br><br>[The above] does not apply to a remedy imposed, enforced, or adopted in accordance with a Party's law following an investigation, inspection, examination, enforcement action, or judicial or administrative proceeding.<br><br>[The above] does not apply to the voluntary transfer of, or granting of access to, source code by a person of the other Party on a commercial basis, such as in the context of a freely negotiated contract.<br><br>For greater certainty, nothing [above] shall prevent a person of a Party from licensing its software on a free and open-source basis. | N/A | Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, including an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.<br><br>For greater certainty, [the above] does not apply to the voluntary transfer of, or granting of access to, source code of software by a person of the other Party, including an algorithm expressed in that source code: (a) on a commercial basis, such as in the context of a freely negotiated contract; or (b) under open source licences, such as in the context of open source coding.<br><br>Nothing in this Article shall preclude a regulatory body or a judicial authority of a Party, or designated conformity assessment body, from requiring a person of the other Party to preserve and make available the source code of software, including an algorithm expressed in that source code, for an investigation, inspection, examination, enforcement action or judicial proceeding, or the monitoring of compliance with codes of conduct and other standards, subject to safeguards against unauthorised disclosure.<br><br>[The above] does not apply to transfers of, or the granting of access to, source code of software, including an algorithm expressed in that source code, for the purpose of the imposition, adoption or enforcement of a remedy granted in accordance with that Party's law following an investigation, inspection, examination, enforcement action or judicial proceeding. |
| **Open Internet Access** | Subject to its applicable policies, laws and regulations, each Party should adopt or maintain appropriate measures to ensure that a consumer in its territory may: (a) access and use services and applications of the consumer's choice available on the Internet, subject to reasonable, transparent and non-discriminatory network management; (b) connect the devices of the consumer's choice to the Internet, provided that such devices do not harm the network; and (c) access information on the network management practices of the consumer's Internet access service supplier. | Subject to their applicable policies, laws, and regulations, the Parties recognise the benefits of consumers in their territories having the ability to: (a) access, distribute, and use services and applications of their choice available on the Internet, subject to reasonable, transparent, and non-discriminatory network management;<br><br>(b) connect devices of their choice to the Internet, provided that these devices do not harm the network; and (c) access information on the network management practices of their Internet access service supplier. | Subject to their applicable policies, laws, and regulations, each Party recognises the benefits of consumers in their territory having the ability to:<br><br>(a) access, distribute, and use services and applications of their choice available on the Internet, subject to reasonable network management which does not block or slow down traffic based on commercial reasons;<br><br>(b) connect devices of their choice to the Internet, provided that these devices do not harm the network; and (c) access information on the network management practices of their Internet access service supplier. | N/A |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Open Government Data** | If a Party chooses to make government information available to the public, it shall endeavour to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused and redistributed.<br><br>The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to and use of government information that the Party has made public, with a view to enhancing and generating business opportunities, especially for small and medium-sized enterprises. | To the extent that a Party chooses to make government information available to the public, it shall endeavour to ensure:<br><br>(a) that the information is appropriately anonymised, contains descriptive metadata, is in a machine-readable and open format, and can be searched, retrieved, used, reused, and redistributed; and<br><br>(b) to the extent practicable, that the information is made available in a spatially enabled format with reliable, easy to use, and freely available application programming interfaces and is regularly updated. | Each Party is encouraged to expand the coverage of government data and information digitally available for public access and use, through engagement and consultation with interested stakeholders, and Māori in the case of New Zealand.<br><br>To the extent that a Party makes government data and information available to the public, it shall endeavour to ensure that the data and information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed.<br><br>Each Party shall provide interested persons with the opportunity to request the disclosure of specific government data and information. | Same as UK-Australia |
| **Financial Services** | | | | |
| **Specific Exceptions** | | Nothing in this Chapter.... shall apply to measures taken or activities conducted by a central bank or monetary authority or by any other public entity in pursuit of monetary policies and related credit policies, or exchange rate policies.<br><br>Nothing in this Chapter shall require a Party to:<br><br>(a) furnish or allow access to information relating to the financial affairs and accounts of individual customers of financial service suppliers or to any confidential or proprietary information which, if disclosed, would impede law enforcement, interfere with specific regulatory or supervisory matters, or would otherwise be contrary to public interest or prejudice legitimate commercial interests of particular enterprises; or<br><br>(b) disclose confidential or proprietary information in the possession of public entities. | This Agreement does not apply to measures taken or activities conducted by a central bank or monetary authority or by any other public entity in pursuit of monetary policies and related credit policies, or exchange rate policies.<br><br>This Agreement does not require a Party to furnish or allow access to information relating to the affairs and accounts of individual consumers, financial service suppliers or to any confidential information which, if disclosed, would interfere with specific regulatory, supervisory, or law enforcement matters, or would otherwise be contrary to public interest or prejudice legitimate commercial interests of particular enterprises. | Nothing in this Chapter shall be construed as preventing a Party, including its public entities, from exclusively conducting or providing activities or services in its territory that form part of a public retirement plan or statutory system of social security, except where those activities may be carried out, by financial service suppliers in competition with public entities or private institutions, as provided by the Party's domestic regulation.<br><br>Nothing in this Agreement applies to activities conducted by a central bank or monetary authority or by any other public entity in pursuit of monetary or exchange rate policies.<br><br>Nothing in this Chapter shall be construed as preventing a Party, including its public entities, from exclusively conducting or providing activities or services in its territory for the account or with the guarantee or using the financial resources of the Party, or its public entities, except where that Party's domestic regulation provides that those activities may be carried out by financial service suppliers in competition with public entities or private institutions. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Prudential Exception** | Nothing in this Agreement shall prevent a Party from adopting or maintaining measures for prudential reasons, including for: (a) the protection of investors, depositors, policy-holders or persons to whom a fiduciary duty is owed by a financial service supplier; or (b) ensuring the integrity and stability of the Party's financial system.<br><br>Where such measures do not conform with this Agreement, they shall not be used as a means of avoiding the Party's obligations under this Agreement.<br><br>Nothing in this Agreement shall be construed as requiring a Party to disclose information relating to the affairs and accounts of individual customers or any confidential or proprietary information in the possession of public entities. | 'prudential reasons' includes the maintenance of the safety, soundness, integrity, or financial responsibility of payment, settlement and clearing systems.<br><br>A Party shall not be prevented from adopting or maintaining measures for prudential reasons, including: (a) the protection of investors, depositors, policy holders, or persons to whom a financial service supplier owes a fiduciary duty<br><br>(b) the maintenance of the safety, soundness, integrity, or financial responsibility of an established financial service supplier or, a cross-border financial service supplier; or<br><br>(c) ensuring the integrity and stability of a Party's financial system.<br><br>Where those measures do not conform with the provisions of this Agreement to which this exception applies, they shall not be used as a means of avoiding the Party's commitments or obligations under those provisions. | 'prudential reasons' includes the maintenance of the safety, soundness, integrity, or financial responsibility of payment, settlement and clearing systems.<br><br>This Agreement does not prevent a Party from adopting or maintaining measures for prudential reasons, including: (a) the protection of investors, depositors, policyholders, or persons to whom a financial service supplier owes a fiduciary duty; (b) the maintenance of the safety, soundness, integrity, or financial responsibility of an established financial service supplier, cross-border financial service supplier, or a financial service supplier; or (c) ensuring the integrity and stability of a Party's financial system.<br><br>Where such measures do not conform with the provisions of this Agreement, they shall not be used as a means of avoiding the Party's commitments or obligations under this Agreement. | Nothing in this Agreement shall be construed to prevent a Party from adopting or maintaining reasonable measures for prudential reasons, such as: (a) the protection of investors, depositors, policy-holders or persons to whom a fiduciary duty is owed by a financial service supplier; (b) the maintenance of the safety, soundness, integrity or financial responsibility of financial service suppliers; or (c) ensuring the integrity and stability of the Party's financial system.<br><br>These measures shall not be more burdensome than necessary to achieve their aim, and shall not constitute a means of arbitrary or unjustifiable discrimination against financial service suppliers of the other Party in comparison to its own like financial service suppliers, or a disguised restriction on trade in services.<br><br>Nothing in this Agreement shall be construed as requiring a Party to disclose information relating to the affairs and accounts of individual consumers or to disclose any confidential or proprietary information in the possession of public entities.<br><br>Each Party shall use its best endeavours to ensure that the Basel Committee's 'Core Principles for Effective Banking Supervision', the standards and principles of the International Association of Insurance Supervisors and the International Organisation of Securities Commissions' 'Objectives and Principles of Securities Regulation', and the internationally agreed Standard for transparency and exchange of information for tax purposes, as spelled out in the 2017 OECD Model Tax Convention on Income and on Capital, are implemented and applied in its territory.<br><br>Subject to Article (National Treatment) and without prejudice to other means of prudential regulation of cross-border trade in financial services, a Party may require the registration or authorisation of cross-border financial service suppliers of the other Party and of financial instruments. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **National Security Exceptions** | Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment or trade in services, nothing in Sections B to F shall be construed as preventing a Party from adopting or enforcing measures which are: (a) necessary to protect public security or public morals or to maintain public order;2 (b) necessary to protect human, animal or plant life or health;3 (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to: (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on contracts; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; or (iii) safety; or (d) inconsistent with paragraphs 1 and 2 of Article 8.8 and paragraph 1 of Article 8.16 provided that the difference in treatment is aimed at ensuring the equitable or effective1 imposition or collection of direct taxes in respect of economic activities, entrepreneurs, services or service suppliers of the other Party. | Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests. | Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it considers contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests. | Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination against the other Party where like conditions prevail, or a disguised restriction on establishment or cross-border supply of services, nothing in this Chapter shall be construed to prevent the adoption or enforcement by a Party of measures: (a) necessary to protect public security or public morals or to maintain public order; (b) necessary to protect human, animal or plant life or health; (c) relating to the conservation of exhaustible natural resources if such measures are applied in conjunction with restrictions on domestic entrepreneurs or on the domestic supply or consumption of services; (d) necessary for the protection of national treasures of artistic, historic or archaeological value; (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter, including those relating to: (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on contracts; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; or (iii) safety; or (f) inconsistent with Article 8.6 (National Treatment) and Article 8.11 (National Treatment), provided that the difference in treatment is aimed at ensuring the effective or equitable imposition or collection of direct taxes in respect of economic activities, entrepreneurs or service suppliers of the other Party. |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Market Access** | A Party shall not maintain or adopt, either on the basis of a territorial subdivision or on the basis of its entire territory, measures that: (a) impose limitations on: (i) the number of service suppliers, whether in the form of numerical quotas, monopolies, exclusive service suppliers or the requirements of an economic needs test; (ii) the total value of service transactions or assets in the form of numerical quotas or the requirement of an economic needs test; or (iii) the total number of service operations or the total quantity of service output expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test; or (b) restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service. | A Party shall not adopt or maintain, with respect to (financial services supplier, investor, cross border financial service supplier), on the basis of its entire territory a measure that imposes limitations on<br><br>(i) the number of established financial service suppliers or crossborder financial service suppliers, whether in the form of numerical quotas, monopolies, exclusive service suppliers, or the requirement of an economic needs test;<br><br>(ii) the total value of financial service transactions or assets in the form of numerical quotas or the requirement of an economic needs test;<br><br>(iii) the total number of financial service operations or the total quantity of financial services output expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test;<br><br>(iv) the participation of foreign capital in terms of maximum percentage limit on foreign shareholding in established financial service suppliers or the total value of individual or aggregate foreign investment in established financial service suppliers; or<br><br>(v) the total number of natural persons that may be employed in a particular financial services sector or that an established financial service supplier or cross-border financial service supplier may employ and who are necessary for, and directly related to, the supply of a specific financial service in the form of numerical quotas or the requirement of an economic needs test; or<br><br>Restricts or requires specific types of legal entity or joint venture through which an established financial service supplier or cross-border financial service supplier may supply a financial service.<br><br>This Article does not prevent a Party imposing terms, conditions, and procedures for the authorisation of the establishment and expansion of a commercial presence provided that they do not circumvent the Party's obligation under [above] and are consistent with the other provisions of this Chapter. | Same as UK-Australia | |

| | UK/Japan CEPA | UK/ Australia | UK/ New Zealand | UK / Singapore |
|---|---|---|---|---|
| **Local Presence** | | Neither Party shall require a cross-border financial service supplier of the other Party to establish or maintain a representative office, or an enterprise or a branch of an enterprise, or to be resident in its territory, as a condition for the cross-border supply of a financial service.<br><br>With respect to cross-border supply as defined in subparagraph (a) of the definition of "crossborder trade in financial services", this Article only applies to the financial services specified by the Party in Annex 9A (Cross-Border Trade in Financial Services) | | |

# Acknowledgements

**Sam Lowe**

Sam Lowe heads Flint's Trade and Market Access Advisory practice. He is a leading European trade expert who regularly advises government officials, parliamentarians, and businesses on issues such as trade in services, digital trade, regulatory barriers to trade, rules of origin, and trade and the environment. He is also a senior visiting research fellow at The Policy Institute, Kings College London.

Sam was previously a member of the UK government's Strategic Trade Advisory Group (2019-2020) and a senior research fellow at the Centre for European Reform, a prominent European think tank. He is regularly asked to provide trade policy analysis in the international broadcast and print media, including the BBC, The New York Times, The Financial Times, and The Economist.

sam.lowe@flint-global.com

**Kathryn Watson**

Kathryn works in Flint's trade policy practice advising clients on political issues and wider policy analysis. Prior to joining Flint, Kathryn was a Commercial Adviser at New Zealand Trade and Enterprise, New Zealand's economic development and trade promotion agency. She has previously worked as an adviser on Brexit and Ministerial Adviser within the New Zealand government.

Kathryn has a Bachelor of Laws from Victoria University in New Zealand.

kathryn.watson@flint-global.com

The City of London Corporation would like to thank everyone who has given their time during the production of this piece of work and contributed to this report.

The views expressed in this paper, and any errors, are those of the authors alone.

Contributors to the Report

**Tehreem Yusuf**
**Global Trade Policy Adviser**
tehreem.yusuf@cityoflondon.gov.uk

**Alexandra Mills**
**Senior Global Trade Policy Adviser**
alexandra.mills@cityoflondon.gov.uk

**Duncan Richardson**
**Head of Global Trade Policy**
duncan.richardson@cityoflondon.gov.uk

**About the City of London Corporation:**

The City of London Corporation is the governing body of the Square Mile dedicated to a vibrant and thriving City, supporting a diverse and sustainable London within a globally successful UK.

We aim to:

- Contribute to a flourishing society
- Support a thriving economy
- Shape outstanding environments
- By strengthening the connections, capacity and character of the City, London and the UK for the benefit of people who live, work and visit here.

cityoflondon.gov.uk

**About Flint Global**

Flint advises business on policy, politics, regulation and competition economics in European and global markets. We help our clients succeed in an increasingly complex world by providing advice at the point where government and business meet, with an authoritative perspective on both.

Members of Flint's expert multi-national team have worked at very senior levels in the British and other European governments, the EU Commission, regulatory agencies, competition bodies and the private sector. Our clients come from many countries and operate in many sectors, including digital, tech, telecoms, media, financial services, life sciences, manufacturing, retail, transport and energy.

flint-global.com