CITY OF LONDON

Past precedent and future opportunities:

assessing digital trade provisions for the UK financial and professional services sector

Contents

Executive summary

Cross-border digital trade has expanded rapidly in recent years. Technological improvements have driven development of new digital products and changing business models. An increasing proportion of global commerce, across all sectors of the economy, is now digitally enabled.

The UK benefits significantly from digital trade in services. Estimates suggest that 67.1% of total UK services exports worth £190.3 billion pre-pandemic were delivered digitally in 2018.[1] The actual figures may be significantly higher and we can assume the global pandemic has further accelerated these trends by pushing an increasing number of business and personal transactions into the digital realm.

Yet, several forces threaten the economic growth opportunities that increased digital trade offers. The rise of digital protectionism increases costs for consumers and businesses.[2] Furthermore, the lack of a global data standard or indeed, any overarching global regulation of digital trade, risks market fragmentation with detrimental impacts for productivity and financial stability.

Against this backdrop, the UK is developing its independent trade policy. At this time of change, the UK has a real opportunity to shape policy in digital trade which takes account of modern realities, lays the foundations for UK-based businesses to succeed, and sets precedent for 21st century trading relationships.

As a starting point, the UK should seek to champion free and open trade in all respects including digital trade. It should use its seat at international fora, including the World Trade Organisation (WTO), and harness the momentum generated by its presidency of the G7 to address the barriers to digital trade.

The UK should combine these efforts with a focus on striking modern bilateral and plurilateral trading relationships. The UK has initiated Free Trade Agreement (FTA) negotiations with Australia, New Zealand, and the USA. Alongside this, it is starting the accession process to the Comprehensive and Progressive Trans- Pacific Partnership (CPTPP) and entering into a Digital Economy Agreement with Singapore. The completed UK-Japan Comprehensive Economic Partnership Agreement (CEPA) laid strong foundations on digital trade which the UK should build upon in these subsequent trade negotiations.

"Cross-border digital trade has expanded rapidly in recent years. Technological improvements have driven development of new digital products and changing business models. An increasing proportion of global commerce, across all sectors of the economy, is now digitally enabled."

1 Cambridge Econometrics, 2020, 'Understanding and measuring cross-border digital trade' available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/885174/Understanding-and-measuring-cross-border-digital-trade.pdf

2 TechUK, 2021, 'A blueprint for UK Digital Trade' available at https://www.techuk.org/resource/a-blueprint-for-uk-digital-trade-a-techuk-report.html

The ultimate aim of these bilateral and plurilateral deals should be to build up to a more digitally focused multilateral system which is fit for purpose and accounts for the recent changes in digital trade.

The UK-based Financial and Professional Services (FPS) sector is inherently international. As such, the free flow of data between various jurisdictions is of paramount importance. Cybersecurity measures, which require a renewed focus in this digital age, often require global solutions which are hampered when jurisdictions have different rules regarding reporting and incidence response. Going forward, it is clear that digital trade policy must consider the impacts of the globalisation of FPS.

This report analyses past precedent in digital trade provisions within FTAs to take stock of what has been achieved in digital trade chapters to date and their particular relevance to the FPS sector. It discusses the mechanisms available to the UK in developing an ambitious digital trade agenda and addressing some of the business issues resulting from a lack of global standards. The report highlights best practice in the form of a case study on Singapore which emphasises what the UK can learn from one of the most modern and forward-looking countries in relation to technology and trade. Finally, the report makes some recommendations as to the UK's future digital trade policy.

This paper aims to initiate a deeper conversation which develops more granular thinking on these issues from across the FPS sector.

"The UK-based Financial and Professional Services sector is inherently international. As such, the free flow of data between various jurisdictions is of paramount importance."

Summary of recommendations

1. **The UK should secure strong commitments from FTA partners to facilitate the cross-border flow of data and information.**

2. **The UK should ensure the free movement of financial data is a feature of all trade agreements going forward.**

3. **The UK should seek to break ground on cooperation between jurisdictions to enhance regulatory coherence and standards in this area.**

4. **The UK should use its seat at the WTO to put forward the case for making the moratorium on e-commerce permanent.**

5. **The UK should seek to use all mechanisms at its disposal to ensure that its digital trade policy is coherent and holistic.**

6. **In order to minimise the issues created by the patchwork of bilateral and plurilateral agreements, the UK should align itself with likeminded jurisdictions and aim to position itself at the heart of an integrated global digital economy.**

7. **The UK should use its trade policy to establish greater cooperation with other jurisdictions on cybersecurity issues.**

8. **Once trade agreements have been signed and ratified, government should assist firms with implementation.**

Introduction

Innovations in digital technologies are transforming and increasing trade in goods and services across all sectors, with connectivity being the new baseline for participation in the global economic system. This increase in digitalisation has made it easier for firms to engage in digital trade which raises a whole set of new challenges, not least how this trade is regulated. One issue is whether the current trade rules adequately address trade in the digital age.

The existing multilateral rules set out by the World Trade Organisation (WTO) were negotiated at a time when digital trade was a nascent concept. Today, firms can flexibly service markets from different locations and their products bundle goods and services making it increasingly difficult to identify the trade rules that apply to specific transactions.[3] As highlighted in a recent paper by the City of London, the benefits of future trade rely on the treatment of services trade and goods trade as interdependent and mutually supportive.[4] The rules-based system which effectively treats these two types of trade as mutually exclusive fails to apply neatly to a system characterised by significant overlaps.

This change, which was underpinned by the rapid rise of globalisation, has been expedited by the global pandemic leading to the exponential growth of digitalisation across all sectors. Slow progress in the multilateral system has seen countries shift their focus to preferential trade agreements as a way of setting the terms of engagement on digital trade. This is likely to increase as technology develops and digital trade becomes the centrepiece of the post-COVID-19 recovery. However, the gaps in the multilateral system must still be addressed.

The rapidly changing nature of technology means that these rules cannot sit in preferential FTAs alone. A range of other mechanisms such as regulatory cooperation, digital economy agreements (DEAs), and memorandums of understanding (MOUs) can further this cause. The ultimate goal of these mechanisms should be to build a more digitally focused multilateral system which is fit for purpose and accounts for the recent changes in digital trade.

"The existing multilateral rules set out by the World Trade Organisation (WTO) were negotiated at a time when digital trade was a nascent concept."

3 OECD (2019), "Trade in the Digital Era", OECD Going Digital Policy Note, OECD, Paris, available at https://www.oecd.org/going-digital/trade-in-the-digitalera.pdf.

4 City of London Corporation (2021),"The City of London: An Ecosystem Enabling International Trade" available at https://www.cityoflondon.gov.uk/supporting-businesses/economic-research/research-publications/an-ecosystem-enabling-international-trade

The UK's digital trade policy

The UK should pursue a forward-looking and modern digital trade agenda using all the mechanisms at its disposal. Only then can the UK forge its way as a leader in digital trade.

Digital trade provisions in recent agreements serve several purposes. They uphold the values of the WTO and provide legal certainty for digital commerce; they lock in digital trade practices and entrench standards which provides businesses with a degree of certainty; they cover issues that have not been discussed in the WTO context; and try to address more contentious areas, such data flows and data protection. The latter of these is where the UK can look to break new ground when pursuing an independent digital trade policy.

So far, the UK has concluded continuity agreements with several countries which roll over the effects of existing EU FTAs. Beyond securing continuity agreements, the UK is also working to secure FTAs with Australia, New Zealand, and the United States (US) and is applying to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Notably with Japan, the UK did not roll over the existing EU-Japan Economic Partnership Agreement (EU- Japan EPA). Instead, the UK negotiated a new enhanced FTA, the UK-Japan Comprehensive Economic Partnership Agreement (CEPA).

The CEPA is the first FTA negotiated and concluded by the UK and thus sets a benchmark for future FTAs. The digital provisions in the CEPA go considerably further than those set out in the EU – Japan EPA. Although there is no separate chapter on digital trade in the CEPA, the provisions included within the services chapter closely mirror those in the United States-Mexico-Canada Agreement (USMCA) and the CPTPP – which have been lauded for the high standard they set in their digital trade chapters. This is a welcome development and helps to cement the UK's position as a forward-looking player in the digital sphere. The CEPA also works towards meeting the digital trade needs of the FPS sector in an FTA. However, an analysis of other recent trade agreements, shows that the UK must include more robust digital trade provisions in its future FTAs if it wishes to position itself as an international leader in digital trade.

This paper maps the key features of specific digital trade provisions in recent agreements (FTAs and DEAs) and identifies their relevance from an FPS perspective. It also provides a comparative analysis of these provisions across seven recent agreements (the examined agreements). These include (1) the CEPA; (2) the US – Japan Digital Trade Agreement; (3) the Digital Economic Partnership Agreement (DEPA); (4) the Singapore – Australia Digital Economy Agreement (SADEA); (5) EU- Japan EPA; (6) the CPTPP; and (7) the USMCA.[5]

This comparative analysis is based on the table in the appendix where the respective texts of these seven agreements have been assessed to identify best practice. The paper goes on to examine the range of mechanisms available to enhance digital trade, the challenges caused by the lack of global standards and how the UK can learn from best practice in other jurisdictions. Finally, the paper presents high level recommendations on what the UK should aim to achieve in its digital trade policy going forward. This paper highlights some outstanding questions for the sector when it comes to digital trade and makes some potential suggestions for next steps. Ultimately it acts as the starting point for a conversation aimed at soliciting granular thinking on these issues from across the FPS sector.

"The UK must include more robust digital trade provisions in its future FTAs if it wishes to position itself as a leader in digital trade."

5 The seven agreements examined in this paper include both FTAs (bilateral, regional and plurilateral) as well as DEAs. Annex 1 provides a comparative overview of the digital trade provisions in these agreements.

Section 1

Provisions on digital trade in recent agreements

Recent FTAs have a number of provisions which lock in good practice when it comes to digital trade. This section highlights precedent in ten different areas. This analysis is based on the comparison table in the appendix:

- **Customs duties**
- **Non-discriminatory treatment of digital products**
- **Domestic regulation**
- **Trade facilitation measures**
- **Consumer protection**
- **Data flows and localisation**
- **Cooperation**
- **Cyber security**
- **Source code**
- **Open government data**

Customs duties

Most agreements covering digital trade include provisions prohibiting the imposition of customs duties on electronic transmissions. This allows for data flows to remain duty free and enables the expansion of digital trade.

These provisions are further bolstered by the WTO moratorium on imposing customs duties on electronic transmissions (the moratorium), which has been supported by WTO members for over two decades. The moratorium is subject to renewal every two years. In 2019, a number of WTO members indicated a desire to end the practice of renewing the moratorium and begin unilaterally imposing tariffs on cross-border data flows. Most notably, India and South Africa have voiced concerns about the loss of revenues that are generated by not imposing tariffs on electronic transmissions.[6]

A United Nations Conference on Trade and Development (UNCTAD) study published in 2019 estimates that the moratorium could prevent countries worldwide from collecting more than $10 billion in tariff revenue.[7] However this has been disputed in an OECD study which states that imposing customs duties on electronic transmissions would cause greater losses to consumer welfare and export competitiveness than any marginal gains in tariff revenues.[8] Proponents of this view argue that the underlying reason to end the moratorium is one of digital protectionism – imposing duties will discourage imports and therefore, local firms can be shielded from competition.

The moratorium was extended temporarily with a view to it being discussed at the 12th WTO Ministerial Conference, which is due to be held in November 2021.[9] Several countries have already called for the moratorium to be made permanent.[10]

6 WTO, "4 June 2019, WT/GC/W/774; WTO, "Work Programme on Electronic Commerce: Moratorium on Customs Duties on Electronic Transmissions: Need for a Re-Think: Communication from India and South Africa," 13 July 2018, WT/GC/W/747.

7 UNCTAD 2019, Growing Trade in Electronic Transmissions: Implications for the South, UNCTAD Research Paper, No. 29, available at https://unctad.org/en/PublicationsLibrary/ser-rp-2019d1_en.pdf.

8 Andrea Andrenelli and Javier Lopez Gonzalez, Electronic Transmissions and International Trade –Shedding New Light on the Moratorium Debate, (Paris: OECD, November 2019), available at https://www.oecd-ilibrary.org/trade/electronic-transmissions-and-international-trade-shedding-new-light-on-the-moratorium-debate_57b50a4b-en.

9 WTO, "Work Programme on Electronic Commerce; General Council Decision of 10 December 2019," 11 December 2019, WT/L/1079.

10 WTO, "Work Programme on Electronic Commerce: Communication from the United States," 28 October 2005, WT/GC/W/551.

RELEVANCE FOR THE FPS SECTOR

The prohibition of customs duties on electronic transmissions provides a cost-effective means for FPS firms to deliver their products across borders. It also provides the necessary confidence and certainty required to build the technology infrastructure of the future. This is especially true of smaller and medium-sized (SME) Fintech firms that are heavily reliant on IT enabled services and would be disproportionately affected by any imposition of customs duties on electronic transmissions. For a smaller payments firm looking to scale up and expand internationally, a duty on each electronic transmission would be prohibitive.

SCOPE IN RECENT AGREEMENTS

As highlighted in the comparative table, provisions prohibiting customs duties on electronic transmissions are included in all of the examined agreements. However, some differences exist in how the obligation is drafted. For example, on the 'product scope', the USMCA states that the prohibition should be applied to digital products transmitted electronically while the other agreements analysed apply the provision to electronic transmissions, including content transmitted electronically. Although different in wording these provisions appear to equally cover all content transmitted electronically.

Further, as concerns the 'geographical scope' of the prohibition for most of the examined agreements, the prohibition only applies to parties to the agreement. However, the EU – Japan EPA adopts a universal application of the prohibition.

The examined agreements also allow parties to impose internal taxes provided that the taxes are imposed consistently with the agreements. However, the US – Japan Digital Trade Agreement and the EU – Japan EPA do not include such a provision.

Non-discriminatory treatment of digital products

Under this provision, imported digital products from one country should not be treated less favourably than other like for like digital products originating from other countries, including the importing country. This is essentially an extension of the principles of national treatment and most-favoured-nation treatment to the digital realm.[11] Equal treatment of digital products ensures healthy competition and provides alternatives to consumers.

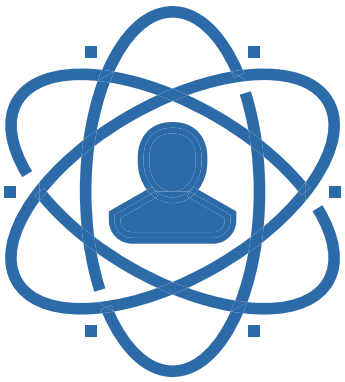
RELEVANCE FOR THE FPS SECTOR

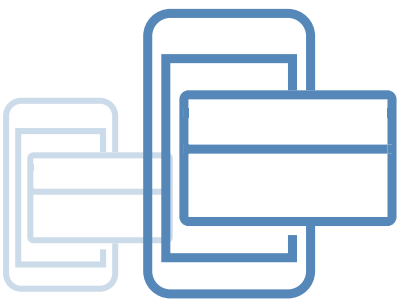
FPS firms benefit from having their products and services treated in a non-discriminatory manner. The immediate benefit is for the firms engaging in cross border trade. However, in the longer term, more robust competition between firms from different jurisdictions leads to lower prices and more diverse and innovative financial systems which ultimately benefits consumers. An additional advantage is the creation of jobs which supports the overall growth of the sector.

SCOPE IN RECENT AGREEMENTS

With the exception of the EU – Japan EPA and the CEPA, all of the examined agreements contain a provision on non-discrimination of like digital products. This applies where the digital products themselves originate from another party or are owned by a person of another party.

The USMCA provision is broader in scope than the other examined agreements since it only exempts subsidies from the application of the obligation. The CPTPP, the DEA, and the DEPA exclude subsidies and broadcasting from the scope of the provision. The US–Japan Digital Agreement carves out measures limiting foreign investment in companies engaged in broadcasting.





11 Wu, Mark. 2017. Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB), available at **https://www.rtaexchange.org/**.

Domestic regulation

Most agreements covering digital trade include provisions requiring parties to maintain a domestic legal framework on electronic transactions. These provisions also require parties to take all efforts to avoid unnecessary regulatory burdens on electronic transmissions and facilitate the participation of interested stakeholders in the development of the domestic legal framework.

RELEVANCE FOR THE FPS SECTOR

Avoiding unnecessary regulatory burdens on electronic transactions makes it easier for FPS firms to operate within other jurisdictions without the need to abide by onerous compliance rules. As firms expand into other markets, it is useful to have clarity on the regulations that apply to cross-border trade. Firms have noted that trade agreements seem to be vague in their commitments on domestic regulation and how these provisions are to be implemented. As domestic regulation is often interlinked to the extent of the cooperation between jurisdictions, greater detail here would be valuable.

SCOPE IN RECENT AGREEMENTS

Of the seven examined agreements, five include binding commitments to maintain rules on electronic transmissions as well as best endeavour commitments to facilitate stakeholder input in the development of those rules and avoid unnecessary regulatory burdens.

The provisions in the EU–Japan EPA and the CEPA adopt a different language requiring parties to administer rules of general application affecting e-commerce in a reasonable, objective and impartial manner. Notably, these commitments do not apply to the content of the rules but rather, to their administration. Although this is a welcome development, as noted above, much greater granularity is required here in order to fully define how these provisions work in practice.

“Firms have noted that trade agreements seem to be vague in their commitments on domestic regulation and how these are to be implemented.”

Trade facilitation measures

These provisions promote the use of technology to facilitate trade. They typically feature commitments for the recognition and adoption of electronic signatures and paperless trading. Under these provisions, parties agree to recognise the legal validity of e-signatures and accept documents submitted electronically as equivalent to their paper versions.

RELEVANCE FOR THE FPS SECTOR

Digital trade facilitation allows greater ease of doing business particularly in relation to conclusion of contracts and invoicing. The delay caused by the requirement of paper documentation can be costly and inefficient. With the increase of remote working and the acceleration of the digitalisation of services trade, due to the COVID-19 pandemic, using digital technologies in business transactions has become the norm. As a result, securing commitments for the adoption and maintenance of digital trade facilitation measures in FTAs and DEAs is now more significant than ever. Digitising a transaction from end-to-end for example would require all participants to be signed up to the same digital solution. In lieu of this standard either platform-neutral solutions or closed-loop solutions among a defined group of participants could enhance interoperability.[12]

SCOPE IN RECENT AGREEMENTS

Trade facilitation measures feature in most of the examined recent agreements. With the exception of the DEPA, all of the examined agreements include provisions requiring parties to recognise the legal validity of e-signatures. The agreements that go furthest (USMCA, CPTPP, SADEA and CEPA) encourage the interoperability of authentication systems but stop short of making any formal commitments.

The comparative table shows that on paperless trading the DEPA and the SADEA push the furthest to enhance and actively promote paperless trade. Indeed, the push towards including binding commitments on paperless trade has traditionally been driven by Australia and New Zealand. By contrast, the provisions in the USMCA and CPTPP adopt best endeavour language which makes the parties' commitments non-binding. The EU–Japan EPA and the CEPA do not include provisions on paperless trading.

12 City of London Corporation (2021),"The City of London: An Ecosystem Enabling International Trade" available at https://www.cityoflondon.gov.uk/supporting-businesses/economic-research/research-publications/an-ecosystem-enabling-international-trade

Consumer protection

Consumer protection provisions typically include commitments to (1) adopt or maintain consumer protection laws against deceptive commercial activities; (2) adopt or maintain rules for the protection of personal information; and (3) limit unsolicited commercial electronic communications.

RELEVANCE FOR THE FPS SECTOR

Consumers ultimately stand to benefit from the increase in the digitalisation of finance. As highlighted in an OECD paper, the benefits of digital financial services include the extension of the potential reach and access of financial services, increased competition and greater choice. However this extension is accompanied by the gathering and storage of huge amounts of personal data. This leads to data protection issues which can encompass uneven levels of protection within and across jurisdictions.[13]

Provisions in trade agreements help to establish and lock in consumer trust in digital trade by establishing consumer protection frameworks.

SCOPE IN RECENT AGREEMENTS

The DEPA provides the gold standard for online consumer protection. It reiterates the commitments made in other FTAs with binding language and more detail such as provisions on adopting and/or maintaining laws to forbid fraudulent conduct. These laws may include general contract or negligence law and may be civil or criminal in nature. The DEPA also requires the adoption of regulations ensuring that goods and services provided are of acceptable and satisfactory quality and availing redress to consumers when they are not.

The most binding commitments on unsolicited commercial electronic communications were originally outlined in the CPTPP which have since been replicated in other FTAs.

On personal data protection, the USMCA and the SADEA align themselves with the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) which includes requirements for the protection of personal information of e-commerce users across the borders of participating APEC countries. Although this issue features prominently in policy debates in the EU, negotiators have not proactively sought such an obligation from their FTA partners. The EU – Japan EPA does not include provisions on the protection of personal information. In contrast, the CEPA requires parties to adopt or maintain laws and regulations on consumer protection.

13 OECD, 2018, 'Financial Consumer Protection Approached in the Digital Age', available at https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf

Data flows and localisation

The growing relevance of data flows across a wide range of sectors of the economy is reflected by the inclusion of provisions on data flows relating to (1) privacy and data protection; (2) cross-border transfer of data by electronic means; and (3) location of computing facilities in most of the recent agreements.

These provisions provide a degree of certainty for firms when conducting business in multiple jurisdictions. Provisions prohibiting restrictions on cross-border data flows such as data localisation lower the financial and operational burden for firms that would otherwise result from storing, processing or replicating data within the jurisdiction where it is generated.

However, in some cases, financial service suppliers – and by extension, financial data – are excluded from the application of provisions on data localisation. This is premised on the view that localisation of financial data is necessary to regulate financial markets and grant access to regulatory and law enforcement bodies, particularly in times of financial crises. This practice became the norm in the wake of the 2008 financial crisis, when US authorities faced difficulties in accessing data stored in Lehman Brothers' servers located in various jurisdictions.[14]

RELEVANCE FOR THE FPS SECTOR

Ensuring that data can flow across borders is a highly pertinent issue for a wide range of subsectors in the FPS sector. Restrictions on the data flows raise operational costs for firms as well as their ability to deliver services to consumers efficiently.

The imposition of localisation requirements raises additional operational costs which limit the competitiveness of foreign financial service suppliers. To meet compliance with localisation, foreign firms must either own or contract out the required local computing infrastructure within every jurisdiction they operate in. These additional costs make foreign financial service suppliers less competitive in foreign markets, especially against local firms that do not compete outside their home markets and therefore do not face the additional costs caused by multiple localisation measures.[15] This cost is often passed on to the consumer. For smaller firms, the ability to operate in a jurisdiction without having to localise their computing operations for financial data would allow them to expand into various markets and avoid any sunk costs.

It also makes it more difficult for FPS firms to fulfil their Anti Money Laundering and Know Your Customer (AML/KYC) requirements when tackling financial crime. These kinds of regulatory functions are best done at a global level to prevent inconsistencies, but varying localisation laws creates challenges in achieving this.

It has further been argued that the rationale for carving out financial services data from provisions on data flows is flawed. Legitimate regulatory concerns are already covered within the wider prudential carve-out (PCO), making any specific carve-out for financial data redundant. The PCO gives national governments the freedom to regulate the financial sector for prudential reasons, notwithstanding any commitments made under the GATS. The PCO is often included in FTAs, but is seen as an 'emergency lever' and therefore not an adequate measure when it comes to data flows in FPS.

A regulator or government can use the carve out for 'legitimate public policy objectives'. If challenged, the issue can be resolved through the dispute resolution mechanisms within the FTA or can be referred to the WTO Appellate Body for resolution. There is also scope for resolution through diplomatic channels or regulator to

14 Cory, N., & Atkinson, R. (2016). Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements, ITIF, available at http://www2.itif.org/2016-financial-data-trade-deals.pdf.

15 Cory, N., & Atkinson, R. (2016). Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements, ITIF, available at http://www2.itif.org/2016-financial-data-trade-deals.pdf.

regulator discussions. However, these procedures can be long and drawn out. Financial regulators often want to be able to access data more frequently and immediately than the PCO allows for which is why jurisdictions opt for a carve out in the digital trade or financial services chapters.

Advocates of data localisation argue that localisation enhances the security of data. However, these benefits are often only advantageous in the short-term. The rise in data localisation may result in firms avoiding certain markets or being forced to set-up or maintain data centres and offices in every jurisdiction they operate within. Furthermore, firms may be hindered from taking advantage of the increased security of global outsourcing providers which may well be greater than those they maintain in their home jurisdiction.

In some cases, localisation requirements allow the cross-border transfer of data but only after the storage of a localised copy of the same. This presents a security risk since data is stored on servers in numerous locations and may be susceptible to malicious attacks.

In addition to this national laws can at times place limitations on what is practically achievable. This can lead to the aspirations for the free flow of data being undercut by local laws which undermine what has been negotiated in the trade agreement. Areas such as employment and consumer protection laws are where nations appear most protective and these areas are often viewed as 'off limits' when it comes to change. Tangentially, firms are sometimes subject to hurdles due to the supervisory approaches in certain markets by home jurisdiction regulators. This may be because of concerns about the potential lack of regulatory supervision once data has left the country. The scope for FTAs to override such supervisory discretion is limited however greater regulatory cooperation could help alleviate some of these issues.

A recent report by the International Regulatory Strategy Group (IRSG) recommends that policymakers should move as close as possible towards mutual recognition of core principles in order to achieve the protection of personal and non-personal data, whilst ensuring the continuation of cross-border trade.[16]

SCOPE IN RECENT AGREEMENTS

With the exception of the EU-Japan EPA, the examined agreements include provisions on data flows prohibiting unnecessary restrictions to the cross-border transfer of information and more specifically, prohibiting data localisation requirements.

With regards to financial data, the SADEA includes financial data within its data flows provision. Crucially for the UK FPS sector, the CEPA sets helpful precedent by explicitly prohibiting restrictions of cross-border flows of data by financial services suppliers. In the CPTPP the provisions of the digital trade chapter apply only to 'covered persons'. Financial institutions are explicitly excluded from the definition given to this term. Accordingly, the prohibition of data localisation requirements does not apply to financial institutions.

The comparative table analyses provisions in the digital trade chapter of the agreements only. But some provisions related to data flows for instance are contained in the financial services chapters of FTAs. In the USMCA for instance, the provisions within the financial services chapter supplement and clarify those contained within the digital trade chapter. Although these provisions ultimately give protection to financial service suppliers, the separate treatment reinforces the idea that financial data should be excluded from provisions on data flows. This may be attributed to how FPS regulators like to access data. The limitations placed

16 International Regulatory Strategy Group (2020) "How the trend towards data localisation is impacting the financial services sector," available at **https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf.**

on data flows in digital trade chapters can be detrimental to regulators' access to data. Therefore, it is included in financial services chapters where the caveats needed can be better defined and the unique relationship the financial services sector has with the regulator can be managed better.

The DEPA allows parties to prevent or limit transfers by a financial institution for reasons relating to the safety, soundness, integrity, or financial responsibility of financial institutions or cross- border financial service suppliers. Although based on prudential reasons, such an exception could have huge implications for financial services providers especially digital payment services necessary for online transactions. It would have to be applied, strictly in a non-discriminatory manner to avoid being used for protectionist motives.

On localisation, the USMCA, the CPTPP, the SADEA, the CEPA, and the DEPA include a carve out for measures that are needed to fulfil a legitimate public policy objective. Further, the US – Japan Digital Trade Agreement and the SADEA go beyond other agreements to include explicit provisions prohibiting localisation of computing facilities for financial services.

The increased fragmentation of the global systems coupled with an increase of protectionist measures mean the complete free flow of data is perhaps an idea of the past. There are added complications in that free flowing data must also meet the condition of upholding intellectual property rights in order to support both innovation and commercial opportunity. However, as the necessary security measures are implemented and developed over time, and as technology progresses, this should allow for data fluidity to a greater extent.

"Policymakers should move as close as possible towards mutual recognition of core principles in order to achieve the protection of personal and non-personal data, whilst ensuring the continuation of cross-border trade." [14]

Cooperation

These provisions include the exchange of information and shared experiences on regulation, policies and enforcement. The more recent agreements seek commitments on cooperation and the maintenance of a dialogue as well as participation in regional and multilateral fora.

RELEVANCE FOR THE FPS SECTOR

Given increased digitalisation and rapidly emerging technologies, regulatory cooperation between trading parties is imperative to address and promote issues such as interoperability and ensure that the digital trade rules function seamlessly across jurisdictions.

SCOPE IN RECENT AGREEMENTS

With the exception of the US – Japan Digital Trade Agreement, provisions on regulatory cooperation are included in all of the examined agreements. However, firm commitments are few and far between. The provisions mainly relate to the exchange of information and the maintenance of regulatory dialogue. Under the USMCA, parties have committed, in non-binding terms, to consider the establishment of a forum to address digital trade issues. Such a forum would offer a unique platform to address issues as they arise which appropriately aligns with the evolving nature of digital technology and the related regulatory concerns.

The comparative table shows that the SADEA and the DEPA offer the best standard since they also include provisions to facilitate cooperation with SMEs. These agreements also initiate an emphasis on the importance of governments collaborating with the private sector to develop initiatives to govern cross-border electronic transactions. The language is often framed around working together to encourage the private sector to adopt codes of conduct, model contracts, guidelines, and enforcement mechanisms.[15]

Annex 8-A on Regulatory Cooperation in Financial Services in the CEPA sets good precedent for the creation of a regulatory forum that promotes a deferential approach. Deference allows authorities in jurisdictions with comparable regulatory, supervisory and/or enforcement standards to promote market access while still effectively overseeing and regulating the cross-border activities of market participants.[18] This is extremely important for cross border financial services trade as it reduces the overlap of duplicative or conflicting regulations and reduces regulatory arbitrage possibilities to improve efficiencies for regulatory authorities and market participants. Although not digital trade specific, the FTA includes a commitment to use this forum to discuss emerging issues in FPS such as diversity in finance and sustainability goals.

A recent paper by the British American Financial Alliance[19] recommends that the "first best solution" would be for trade agreements to include provisions establishing a framework for a regulatory cooperation forum to foster opportunities for stakeholder engagement and transparency.

Similar to Annex 8-A of the CEPA, these provisions should clarify that the decisions of this regulatory forum would not be subject to the dispute settlement provisions of the trade agreement. The organisation and governance of the regulatory cooperation forum should be established outside of the trade text, in a separate understanding. Finally, the forum should have a clear mandate to consider and resolve unintended market access barriers to the greatest extent possible while maintaining high prudential outcomes.

17 Wu, Mark. 2017. Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB), available at https://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf.

18 IOSCO (2020), "Good Practices on Processes for Deference", available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD659.pdf

19 British American Finance Alliance, (2020) "Scoping Paper on Formalizing U.K.–U.S. Regulatory Dialogue," available at https://www.sifma.org/wp-content/uploads/2020/09/British-American-Finance-Alliance-Scoping-paper-on-formalizing-UK-U.S.-regulatory-dialogue.pdf

Cybersecurity

Provisions on cybersecurity include a commitment to build capabilities responsible for incidence response and strengthening collaboration on risk-based approaches and preventative practices. The adoption of risk-based measures to address cyber threats is preferred over prescriptive regulation which can become outdated in view of how quickly digital technologies and the related threats evolve.[20]

RELEVANCE FOR THE FPS SECTOR

Increased digitalisation leaves businesses and particularly FPS firms open to risks of cyber attacks. This is a global problem but despite the global financial system's increasing reliance on digital infrastructure, it is unclear who is responsible for protecting the system against cyber attack. A recent paper by the Carnegie Endowment for International Peace highlights that greater clarity about roles and responsibilities is required and that international collaboration is necessary and urgent. The paper argues that reducing fragmentation will free up capacity to tackle the problem posed by cyber threats and rather than duplicate efforts, actors should seek to better coordinate and internationalise mature and effective initiatives.[21]

It is therefore imperative to build in cooperation on cybersecurity issues within trade agreements as they can lead to consensus-based standards. Furthermore, risk management best practices are required to help minimise risks. Firms have expressed that greater specificity in responding to cyber issues rather than just maintaining a dialogue would be of utmost value.

SCOPE IN RECENT AGREEMENTS

The examined agreements include provisions on cybersecurity. However, the content varies across agreements. With the exception of the EU-Japan EPA and the CEPA, which only set out commitments to maintain a dialogue, these provisions typically focus on building capabilities for cybersecurity incident response; and cooperation to identify and mitigate malicious cyber activities that affect the electronic networks. Besides this, the DEPA and the SADEA emphasise the need for workforce development in cybersecurity.

The USMCA and the US – Japan Digital Trade Agreement offer a better standard insofar as they include a recognition of the importance of taking a risk-based approach to cybersecurity instead of prescriptive approaches, including risk-based approaches that rely on consensus-based international standards and best practices.

"Firms have expressed that greater specificity in responding to cyber issues rather than just maintaining a dialogue would be of utmost value."

20 Meltzer, J. P. (2020). Cybersecurity, Digital Trade, and Data Flows: Re-thinking a Role for International Trade Rules. Global Economy & Development WP, 132.

21 Carnegie Endowment for International Peace (2020), "International Strategy to Better Protect the Financial System Against Cyber Threats" available at **https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf**

Source code

Source code of software or an algorithm expressed in the source code typically contain information that grants a competitive advantage to the party owning it. Most of the agreements covering digital trade include provisions prohibiting the forced transfer of source code or software owned by a person of another party as a condition for market access. Some agreements extend this to cover algorithms, and encryption keys. These provisions are aimed at ensuring security for businesses, reducing risk of theft and piracy, and removing trade barriers.

RELEVANCE FOR THE FPS SECTOR

These provisions are of value to Fintechs as source code is often at the heart of their business. The protection of this intellectual property, which in some cases may give firms a competitive advantage over other players in the market, is important to safeguard the ultimate survival and effectiveness of the business.

SCOPE IN RECENT AGREEMENTS

With the exception of the DEPA, all of the examined agreements include a prohibition on forced transfer of access to source code as a condition for market access. The USMCA, the CEPA, the SADEA, and the US – Japan Digital Trade Agreement go a step further and extend this protection to algorithms.

In addition, the examined agreements include exceptions that allow regulatory bodies or judicial authorities to require access to source code for an investigation, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure. Further the CEPA, the CPTPP and the SADEA include provisions that allow businesses to voluntarily transfer or grant access to source code through contractual arrangements.

As highlighted in the comparative table, the CPTPP, includes an additional provision, limiting the prohibition to mass market software or products containing such software and does not include software used for critical infrastructure. While the DEPA does not include a provision for protection of source code, it incorporates provisions for protection of encryption (ICT products that use cryptography).

Open government data

These provisions are relatively new within FTAs and allow for government data to be made public. Governmental bodies produce and commission large quantities of data and information. Making their data sets available can generate and enhance business opportunities for firms who require these datasets to test and develop their products. This provision goes hand in hand with the development of Artificial Intelligence (AI) as access to large data sources are crucial to train AI programs.

RELEVANCE FOR THE FPS SECTOR

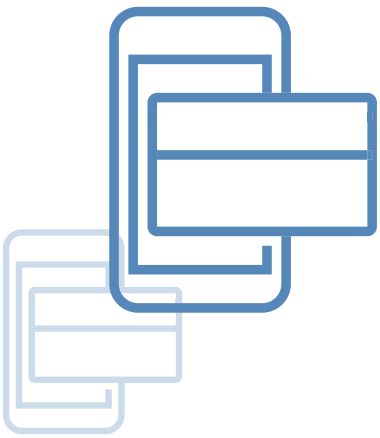
Access to government data encourages the use, reuse and free distribution of datasets. FinTechs in particular would benefit from the ability to use real data sets when testing their products.

SCOPE IN RECENT AGREEMENTS

With the exception of the EU – Japan EPA and the CPTPP, the examined agreements include provisions on the use of open government data emphasising the benefits of access to and use of government data on innovation, competitiveness, and economic development.

The USMCA provides the gold standard here by committing parties to make government data available to the public. This is in formats which can be searched used and redistributed.

These provisions typically include a non-binding, best-endeavour commitment to provide government data in a machine-readable and open format that can be searched, retrieved, used, reused and redistributed.



Summary table of provisions – a full analysis can be found in the Appendix.

Provision	Analysis
Customs Duties	All the examined agreements include provisions prohibiting the imposition of customs duties in electronic transmissions.
Non-Discriminatory treatment of digital products	With the exception of the EU-Japan EPA and the CEPA, all the examined agreements contain a provision on non-discrimination of like digital products.
Domestic Regulation	The majority of agreements (with the exception of the EPA and the CEPA) include binding commitments to maintain rules on electronic transmissions as well as best endeavour commitments to facilitate stakeholder input in the development of those rules and avoid unnecessary regulatory burdens.
E-Signatures	Nearly all agreements include provisions for the acceptance of e-signatures. Those that go further encourage the interoperability of systems, but make no formal commitments. The EU has historically adopted a more light touch approach to the acceptance of e- signatures, not often requiring firm commitments. However the recent EU-Japan EPA is in line with the more forward looking agreements. The CEPA goes further still by encouraging the use of interoperable electronic authentication and e-signatures.
Paperless trading	The USMCA and the CPTPP include provisions that require soft commitments. The DEPA and the SADEA push further to enhance and actively promote paperless trade. Indeed, the push towards including commitments, especially binding ones, on paperless trade has been driven traditionally by Australia and New Zealand. For the EU a provision on paperless trading is not found in most agreements. The US does not include this provision in all agreements, but has done most recently.
Online Consumer Protection	The DEPA provides the current gold standard of what is achievable in online consumer protection. It reiterates the commitments made in the other trade agreements with stronger wording and more detail. Within EU FTAs the primary emphasis is usually on regulatory dialogue for consumer protection – the wording of provisions is often softer. Although the CEPA goes beyond the EPA, it still falls short of the firmer commitments made in some of the other agreements which espouse the adoption or maintenance of a legal framework for consumer protection.
Unsolicited Commercial Electronic Communications	The CPTPP originally outlined the most binding commitments which have then been replicated in other trade agreements.
Protection of Personal Information	The USMCA and the SADEA align themselves with the APEC Cross Border Privacy Rules which include requirements for the protection of personal information of users of e-commerce and has among its aims the protection of the data of individual natural persons in e-commerce. The CBPR was first established in 2011 by the Asia-Pacific Economic Cooperation (APEC)—a "regional economic forum" of 21 Asian-Pacific member economies. Like the European Union's General Data Protection Regulation (GDPR), the CBPR also governs the transfer of personal information across the borders of participating countries. The DEPA goes further than the others by having slightly stronger wording on interoperability cooperation as well as provisions for trustmarks. Although this issue features prominently in policy debates in the EU, negotiators have not proactively sought such an obligation from their FTA partners. Provisions within the CEPA have gone beyond those in the EU-Japan EPA and are on a par with the provisions within the USMCA and the CPTPP.

Provision	Analysis
Data Flows	Some provisions related to data flows are contained within both the digital trade and financial services chapters in trade agreements. In the USMCA for instance the provisions within the financial services chapter supplement and clarify those contained within the digital trade chapter. Within the CPTPP, a covered person does not cover financial institutions. This has huge implications for financial services providers especially digital payment services necessary for online transactions. The DEPA allows parties to prevent or limit transfers by a financial institution for reasons relating to the safety, soundness, integrity, or financial responsibility of financial institutions or cross- border financial service suppliers. This however does not apply to electronic payments. Unsurprisingly, agreements with Singapore seem to be the most forward looking. The SADEA includes financial data within data flows provision as does the CEPA which was seen as a welcome development by the UK FPS industry.
Data Localisation	The USMCA, the CPTPP, the CEPA and the DEPA text caveat the provisions with a carve out for legitimate public policy objectives. This is not contained within the USMCA. US-Japan includes a specific provision for financial services which goes beyond the USMCA. In contrast the SADEA carves out FS.The provision in the CEPA is similar to that contained in the USMCA.
Location of Financial Services Computing Facilities for Covred Financial Services Suppliers	The US - Japan Digital Trade Agreement and SADEA include an explicit provision prohibiting localisation for financial service suppliers.
Cooperation	The emphasis on regulatory dialogue is contained within most provisions. In many trade agreements in the Asia Pacific region, there is a provision to facilitate the use of e-commerce for SMEs. These trade agreements also initiated an emphasis on the importance of governments collaborating with the private sector to develop initiatives to govern cross border electronic transactions.
Cybersecurity	The EU - Japan EPA has a light touch approach here. The DEPA and the SADEA are more comprehensive insofar as they recognise the importance of workforce development in this area.
Source Code	The USMCA, like the CPTPP, stipulates that governments cannot force companies to the disclose source code in order to enter a market . The USMCA, the CEPA, the SADEA, UK-Japan Digital Trade Agreement go a step further and extend this protection to algorithms. The CPTPP is limited to mass-market software and does not include critical infrastructure.
SMEs	All of the trade agreements make mention of SMEs and helping to facilitate their use of e-commerce. The DEPA, EU-Japan and the SADEA include specific chapters/modules on SMEs with EU-Japan providing a one point 'helpdesk' for SMEs and the DEPA committing to convening an Digital SME Dialogue.
Open Government Data	Access to open government data is a relatively new provision which goes hand in hand with the development of AI as access to large data sources are crucial to train AI programs. The USMCA has set a gold standard that commits parties to make government data available to the public in machine-readable and searchable open formats, and allow it to be searched, retrieved, used, reused, and redistributed. This is replicated in the DEPA and the SADEA.

Section 2

Provisions that sit outside digital trade chapters

Provisions that sit outside digital trade chapters

Some provisions related to the FPS sector sit outside of digital trade chapters, most notably in the financial services chapter of trade agreements. As explained above, the USMCA excludes financial institutions from the scope of the data flow provisions. However, this is supplemented by a provision within the financial services chapter which allows for the cross-border transfer of information by electronic or other means when this activity is for the conduct of business within the scope of the license, authorisation, or registration of a financial institution.

This raises a question on the location of provisions pertaining to the digital trade of financial services. It could be argued that the importance of data for the FPS sector as well as the specific detail required when it comes to FPS cross-border trade mean that these provisions should sit within the financial services chapter albeit, supplementing what already exists within the digital trade chapter.

As is the case for services trade more broadly, ongoing regulatory cooperation is invaluable in making effective gains in the digital trade space. These can ensure that important issues are discussed on a regular basis and any regulatory changes are aligned or at least deemed to work alongside the regulation of another jurisdiction.

Annex 8-A on Regulatory Cooperation in Financial Services in the CEPA sets good precedent for the creation of a regulatory forum that promotes deference for regulation and encourages policymakers to work to avoid duplicative, unnecessarily burdensome, and divergent regulation. This annex provides a framework to discuss the digital trade agenda in FPS and firms have noted that they will follow the establishment procedures of this forum closely.

Aside from the provisions contained in FTAs specifically there are a range of other mechanisms that can be used to further ease digital trade. DEAs that sit along formal FTAs are valuable for the UK when engaging in rollover FTA agreements. In the case of Singapore the UK has rolled over the FTA and has signalled its intention to negotiate a DEA which will seek to go beyond the digital trade provisions that already exist.

Focused agreements are useful when it comes to negotiations since there is no need for trade-offs with other topics. In breaking away from the traditional FTA framework, DEAs keep digital trade issues from being used as 'bargaining chips' or compromised in favour of interests in other sectors. Arguably, this keeps the focus on designing digital trade rules that truly match the current global realities. Further, the exclusion of other trade issues allows for some flexibilities with respect to the review of the rules.

Although DEAs and FTAs are interlinked – the wording of the former being enshrined in the latter – there is a degree of flexibility within DEAs which is valuable. With the use of MOUs and side agreements, the DEA can be built upon and modified as digital trade becomes increasingly advanced.

"Ongoing regulatory cooperation is invaluable in making effective gains in the digital trade space."

As the UK pursues its digital trade agenda it is important that it uses all the tools at its disposal to make digital trade easier for firms and produce a coherent and holistic digital trade policy. Recent agreements present numerous examples of best practice and it is important that the UK follows these precedents as a first step in its digital trade policy ahead of seeking to develop more innovative provisions.

It is important to note that agreements made with other jurisdictions on rules to define digital trade present the first step in addressing barriers for firms. These provisions then must be understood and implemented by firms whilst minimising disruption to their day to day practices. This is particularly true for SMEs which sometimes require additional support to take advantage of provisions agreed. Clear and consistent messaging on how this can be achieved is invaluable for firms in this implementation process. Government messaging can be tailored in a more business-friendly way to improve engagement with UK businesses. This includes clearer signposting of business-facing guidance and announcements and making it easier for UK businesses to participate in UK Government-sponsored initiatives such as trade missions.[22]

In applying to accede to the CPTPP, the UK has signified that it values and will uphold modern digital trade provisions. To help cement the UK's position at the heart of the global digital economy the UK should also seek to join the DEPA. As the UK is pursuing bilateral deals with two of the three signatories of the DEPA (an FTA with New Zealand and a DEA with Singapore), it could be argued that there is little to be achieved economically through joining the DEPA. However, the benefit of joining the DEPA comes from being at the forefront of developments in digital trade. This could perhaps pave the way for other jurisdictions to join the DEPA thereby creating a coalition of likeminded jurisdictions agreeing to uphold many of the gold standard of provisions in digital trade.

Given the CPTPP contains many more countries than the DEPA, joining the latter may prove to be a simpler process. As the current members of the DEPA have agreed to uphold the provisions within the CPTPP, joining the DEPA would assist the UK in its accession.

22 City of London Corporation (2021),"The City of London: An Ecosystem Enabling International Trade" available at https://www.cityoflondon.gov.uk/supporting-businesses/economic-research/research-publications/an-ecosystem-enabling-international-trade

"As the UK pursues its digital trade agenda it is important that it uses all the tools at its disposal to make digital trade easier for firms and essentially produce a coherent and holistic digital trade policy."

Section 3

The absence of global standards

The absence of global standards

The prevalence of bilateral deals when it comes to digital trade have been both the cause and the effect of the lack of global standards in this field. The absence of any overarching global regulatory guidelines on baseline provisions for digital trade have led to greater adherence to bilateral and plurilateral solutions.

However, the resulting fragmentation across the global digital economy is becoming increasingly problematic. UK FPS firms are concerned that a patchwork of different agreements across a range of jurisdictions will make cross-border digital trade more difficult from a business perspective. The UK has made a good start with the CEPA as well as its desire to accede to the CPTPP, but the forward-looking nature of these agreements should have the ultimate goal of building back towards developing a more digitally focused multilateral system.

Questions on how best to regulate the global digital economy have existed for several years and the lack of development in this area is a strong indication of the complexity of this task. Developments at the WTO level have been slow and infrequent. This is in part due to the WTO's size and the inherent difficulties that come from attempting to achieve consensus across 150 very diverse economies. Indeed, the multilateral rules on cross border electronic transactions have not been meaningfully updated since the General Agreement on Trade in Services (GATS) entered into force in 1995. There is hope however that the negotiations on the Joint Statement Initiative on Electronic commerce (JSI) which were launched in 2019 will fill this gap and update the regulatory framework for the digital economy. A breakthrough here would be welcomed by industry.

The UK has taken steps to participate in this initiative by submitting text proposals on a number of key topics including customs duties on electronic transmissions, personal information protection, cross-border transfer of information, location of computing (and financial computing) services, source code, cryptography, open internet access, cybersecurity, electronic contracts, and paperless trading.[23]

The UK should use its G7 presidency to push solutions forward. As highlighted in a recent IRSG paper on the financial services priorities for the UK's G7 presidency, there is an opportunity for the UK to promote greater international consistency around privacy regulation as this would greatly facilitate global data flows. [24] If the failure of the WTO can in part be attributed to its size then the G7, a grouping of likeminded , similar sized economies should provide a much more appropriate forum to discuss these issues and reach consensus.

Greater consistency stems from uniformity of both standards and practice. The former, e.g. a global data standard, is something which the UK can take steps toward by joining with likeminded jurisdictions within the G7. However, it should be recognised that although a global standard is the ultimate goal, it may well prove to be an unattainable one given the size of the task and the differences in approach across jurisdictions. This is further complicated by the fact that even global standards are subject to differences in interpretation, enforcement, and national supervision.

This is not to say that a global standard should not be the ideal, but rather, it is the steps taken to get there that are equally as important as the end goal.

Initiatives to encourage the interoperability of existing systems are a key factor here. In the absence of a global standard it is essential that various systems can co-exist in a coherent manner. This assists firms when having to deal with the regulation of various jurisdictions and should encourage convergence over time.

Other possible initiatives include a digital trade taxonomy which will help identify and define aspects of digital trade and simplify this for firms. In financial services this is of particular relevance given the importance of issues such as financial data - a term which has no set definition when it comes to cross-border trade. Here the sector as well as the government has a role to play in assessing which terms it would be useful to define versus terms

23 Julian Braithwaite, UK Ambassador to the WTO in Geneva, statement during the WTO Joint Initiative on E-Commerce plenary session, (2020), available at https://www.gov.uk/government/speeches/uk-statement-for-joint-initiative-on-e-commerce-plenary-session

24 IRSG (2021), "Financial services priorities for the UK's G7 presidency" available at https://www.irsg.co.uk/resources-and-commentary/financial-services-priorities-for-the-uks-g7-presidency/

where it would be valuable to allow a greater degree of fluidity or indeed where over prescribing may prove an inhibitor to trade. The same is true of how jurisdictions define what is a financial institution or supplier. The US classification of financial institution does not cover the likes of Apple Pay for instance which is problematic. Tech companies are effectively able to provide financial services without being regulated as a financial institution would be. Furthermore, there are privacy concerns around the financial data collected through services such as these.

In the FPS sector there are certainly some aspects of financial data which are deemed more important than others when it comes to cross border trade. At the very least, defining which types of data are a priority when it comes to FPS trade will be useful when engaging in trade negotiations as well as when defining the broader UK digital trade policy objectives in relation to the FPS sector.

As well as addressing some outstanding issues as highlighted above, there must be a renewed focus on cyber threats in the face of the increased digitalisation of the sector. Regulators need to be able to follow transactions. As such, access to data is critical to ensure the stability to the FPS sector via good risk management. As these threats are global in nature, the response too must be global. Greater information sharing and identifying best practice when it comes to response are ways in which the UK can increase its preparedness as digitalisation accelerates.

The UK should look to jurisdictions which have made a great deal of progress in these areas in recent years. The Singaporean example is one that the UK can draw on not only for innovations in digital trade but also as a trailblazer when it comes to operational resilience in the face of growing digitalisation.

"The UK has made a good start with the CEPA as well as its desire to accede to the CPTPP, but the forward-looking nature of these agreements should have the ultimate goal of building back towards developing a more digitally focused multilateral system."

Section 4

What does best practice look like? Case Study: Singapore

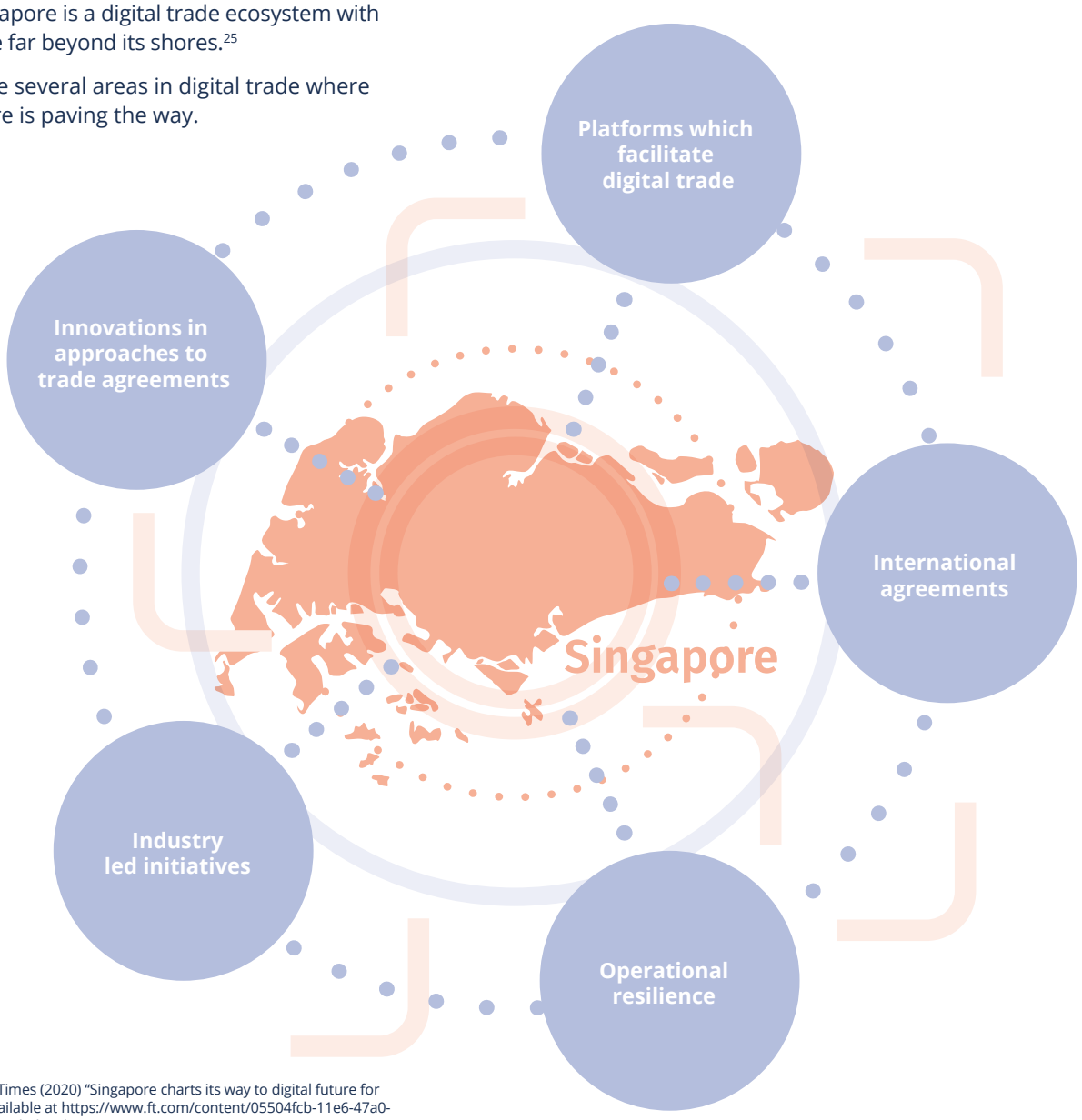
There are several areas in digital trade where Singapore is paving the way.

- **Innovations in approaches to trade agreements**
- **Platforms which facilitate digital trade**
- **Industry led initiatives**
- **Operational resilience**
- **International agreements**

The UK signed a rollover agreement with Singapore which came into effect in January 2021. The digital aspects of this agreement however will be developed and updated in the UK-Singapore DEA which is currently being scoped with the aim of launching negotiations in Summer 2021.

Policymakers in Singapore see digitalisation as a necessary tool for future cross-border trade and are taking advantage of the increasing adoption of e-commerce. Its advanced thinking in seeking to align trade rules and standards across its neighbouring jurisdictions and beyond means that Singapore is a digital trade ecosystem with influence far beyond its shores.[25]

There are several areas in digital trade where Singapore is paving the way.



25 Financial Times (2020) "Singapore charts its way to digital future for trade," available at https://www.ft.com/content/05504fcb-11e6-47a0-8860-7d156d1d82ab

Innovations in approaches to trade agreements

As this analysis confirms, Singapore's agreements – the DEPA and SADEA – contain some of the most forward-looking provisions on digital trade. The DEA framework seeks to align digital rules and standards and encourage interoperability.

The DEPA on the other hand presents a novel way for members to engage in digital trade. It sets out a series of modules which cover a range of emerging digital economy issues and topics of relevance to FPS firms. These modules are intended to be building blocks for future agreements on digital trade. The DEPA is open to accession by other countries. Alternatively, to increase the significance of the DEPA, countries can adopt its modules in other FTAs or domestic policies.[26] These modules include a number of areas that have never before formed a part of trade agreement, such as digital identities and digital inclusion.

The way in which Singapore approaches cross border digital trade seeks to step away from the more static FTA framework in favour of greater flexibility which recognises the rapidly changing nature of technology.

Platforms which facilitate digital trade

Business Sans Border which allows SME centric digital hubs to connect to similar hubs in other jurisdictions to enable businesses to sell their services in a much larger marketplace.[27]

Trade Trust, a global digital platform which uses blockchain technology to digitalise international ecommerce.[28]

Contour which seeks to effectively digitise the methods around trade finance which are traditionally paper and process driven.[29]

Industry led initiatives

Singapore Together Alliances for Action (AfAs) These are industry-led coalitions that work in partnership with the government to seize growth opportunities for Singapore. A particular focus is on the digitalisation of global supply chains which has long been hampered by low adoption, lack of data sharing, and the prevalence of existing platforms. With stronger concerns about supply chain resilience in a post-COVID world, there will be increased demand for end-to-end adoption.

26 Unpacking the Digital Economy Partnership Agreement (DEPA), available at http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa.

27 More information can be found at https://www.mas.gov.sg/development/fintech/business-sans-borders

28 More information can be found at https://www.tradetrust.io/

29 More information can be found at https://www.contour.network/

Operational resilience

In the face of increasing digitalisation, Singapore is taking steps to mitigate the risks posed by cyber threats and to ensure operational resilience.

- As well as regular stress testing and inspections of financial institutions, regulators recommend legislative as well as non-legislative initiatives. Aside from the compulsory set of cyber security measures which all financial institutions must abide by, authorities have introduced standards and guidelines to promote security amongst cloud service providers for instance.
- Cyber security capability grants are available to help financial institutions develop and implement security measures.

Domestic regulation and standards are supplemented with cross border collaboration:

- Participation in the Financial Stability Board Singapore is a member of the FSB's cyber lexicon working group which has developed 50 core terms related to cyber security and cyber resilience in the financial sector. This is intended to support the work of the FSB, standard-setting bodies, authorities and private sector participants, e.g. financial institutions and international standards organisations, to address financial sector cyber resilience.
- Singapore is also part of the Financial Services Information Sharing Analysis Centre (FSISAC). This is the only cyber intelligence information sharing group which focuses on FPS sector. Their aim is to launch an information sharing forum for central banks regulators and supervisors to let members exchange best practice and information on vulnerabilities.

International agreements

Singapore signed a statement of intent with the US Treasury committing to collaboration on the avoidance of localisation measures. Whilst recognising the risks for policymakers and regulators posed by the expanding use of data in financial services, the US and Singapore have committed to work together and with other countries to promote an environment in financial services that fosters the development of the global economy.[30]

30 USTR, (2020) United States – Singapore Joint Statement on Financial Services Data Connectivity, available at https://home.treasury.gov/news/press-releases/sm899

Section 5

Recommendations

The UK government has made it clear that it wants to adopt modern and forward-looking digital trade provisions in its trade agreements with other jurisdictions. The success of this would bring real benefits for the FPS sector which in turn is a huge driver of national and global prosperity. There are numerous ways in which this can be achieved – through trade mechanisms, regulatory cooperation, and from following best practice examples from jurisdictions such as Singapore. In conjunction with this, the UK government and industry need to work collaboratively to unpack areas where firms could be better equipped to engage in cross border digital trade. These initiatives could take the form of better regulation or enhanced security measures, with the outlook being both national and global in remit. Below are some initial steps the UK can take to ensure a coherent and effective digital trade policy from an FPS perspective.

Recommendations

1. The UK should secure strong commitments from FTA partners to facilitate the cross-border flow of data and information.

For FPS firms any FTAs that do not include these provisions are problematic. This is in part due to the increased costs associated with operating in those markets where data localisation measures are imposed but more importantly as it detracts from the certainty around doing business. While many jurisdictions do not restrict cross-border data flows, having this provision formally included within a trade agreement guarantees security and predictability for firms.

Although increased fragmentation and the rise of digital protectionism mean that the future of the complete free flow of data looks uncertain, the UK should seek to explore and develop the technical or regulatory security mechanisms which can reduce if not remove the barriers posed by some limits on the free flow of data.

It is also worth mentioning that calling for the free flow of data is not meant with the intention of impinging on the intellectual property rights which ultimately facilitate invention. The free flow of data should be supported alongside other initiatives which encourage innovation and commercial opportunity.

2. The UK should ensure the free movement of financial data is a feature of all trade agreements going forward.

The benefits of this for FPS firms, particularly smaller firms which would like to test operations within a market are profound. The security issues that are cited as the justification for broader data localisation are often offset by the risks and costs of having to store data across multiple sites. Ultimately, this reduces international competition between firms and raises costs for consumers. As discussed above, the concept of financial data is not defined and defining it could unintentionally inhibit trade. The question therefore remains as to which types of financial data are of the utmost importance for the FPS sector and if these vary by subsector. Government should seek to work with industry to identify these data types in order to garner an understanding of where their efforts are best placed when it comes to trade negotiations.

3. The UK should seek to break ground on cooperation between jurisdictions to enhance regulatory coherence and standards in this area.

This includes using multilateral fora to promote and enhance interoperability. Related to this is the issue of domestic regulation. Although many jurisdictions commit to the avoidance of unnecessary regulatory burdens on electronic transmissions, firms have noted that greater detail and more prescriptive provisions here would be valuable.

The balkanisation of the internet and digital trade is problematic and increasing divergence in approaches from key players such as the EU and the US compound this issue. The UK could act to bridge the gap between these differences in a bid to encourage greater convergence over time.

4. The UK should use its seat at the WTO to put forward the case for making the moratorium on e-commerce permanent.

This offers certainty for businesses which can then plan and build the necessary infrastructure required in the development of innovative digital trade policies.

For the FPS sector, prohibition of customs duties on digital trade allows for information flows to remain duty free and leads to the expansion of digital trade. Several countries have already called for the e-commerce moratorium to be made permanent. For businesses this provides the necessary confidence to build the technology infrastructure of the future.

5. The UK should seek to use all mechanisms at its disposal to ensure that its digital trade policy is coherent and holistic.

Digital trade chapters within FTAs should be complemented with more sector specific provisions within financial services chapters. DEAs offer a degree of flexibility as they can be supplemented with MOUs and side agreements which can be updated and changed as technology evolves. The UK is the first jurisdiction outside of the APAC and Association of Southeast Asian Nations region to engage in a DEA negotiation the culmination of which will help cement the UK's position as a likeminded partner to the most forward looking and modern digitally trading nations.

The UK should seek to join the DEPA, if not for the economic benefits, but for the fact that it represents a novel framework for agreeing rules on cross border digital trade and the UK would benefit from being at the forefront of this innovation. The formal mechanisms mentioned here should also be supplemented with regulatory dialogue and discussion over slower time in order to achieve greater levels of convergence over time.

6. In order to minimise the issues created by the patchwork of bilateral and plurilateral agreements, the UK should align itself with likeminded jurisdictions and aim to position itself at the heart of an integrated global digital economy.

The UK has already made headway here in terms of the trade negotiations to date. The UK can also push this agenda forward through its G7 presidency. The G7 is ideally placed to encourage progress in this area given the ability of a relatively small number of like-minded jurisdictions to set the standard on what good looks like and to broker a core critical high-level commitment globally.[31]

7. The UK should establish greater cooperation on cybersecurity issues.

This can be achieved through the sharing of information and best practices, with a view to improve on the identification and mitigation of cybersecurity threats. This includes learning from best practice, regulator to regulator dialogue, MOUs on cyber security cooperation as well as taking part in multilateral efforts to quell threats.

8. Once trade agreements have been signed and ratified, government should assist firms with implementation.

This includes in understanding what these provisions mean for their business in practical terms and how to take full advantage of them. The implementation of provisions is particularly important for SMEs which may need additional support in utilising the trade provisions but in some cases will stand to reap the greatest benefit.

31 IRSG (2021), "Financial services priorities for the UK's G7 presidency" available at https://www.irsg.co.uk/resources-and-commentary/financial-services-priorities-for-the-uks-g7-presidency/

Conclusion

As concerns digital trade provisions, the UK is moving in the right direction. In particular, the provisions on data flows in the CEPA are considered by industry as a welcome improvement on the EU–Japan EPA.

However, for the UK to forge ahead in digital trade rules, it needs to look beyond a comparison of its provisions with the EU's position and examine other provisions in recent agreements within the APAC region and the US. These provisions along with the help of other mechanisms such as regulatory dialogue will help foster the smoother functioning of the digital economy and provide regulatory certainty for businesses.

This paper has highlighted some outstanding issues that exist for the FPS sector pertaining to global standards, taxonomy and data, and potential solutions that can be explored. This list is far from exhaustive and the aim of this paper has been to act as the conversation starter for further collaborative granular thinking on these issues across government and industry. This will assist in the furthering the development of the UK's digital trade policy in a way that caters to the requirements of the FPS sector.

Appendix *Comparative table of key provisions relevant to FPS in recent agreements*

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Digital Trade Provisions/Parties	US, Mexico and Canada	US, Japan	Canada, Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam	New Zealand, Chile and Singapore	Singapore, Australia (upgrades arrangements Australia and Singapore made under CPTPP)	EU, Japan	UK, Japan
Customs duties	No customs duties on digital products transmitted electronically. However, parties are not precluded from imposing internal taxes.	No customs duties on electronic transmissions, including content transmitted electronically. However, parties are not precluded from imposing internal taxes.					
Non-discriminatory treatment of digital products	No less favourable treatment for like digital products from other jurisdictions. This applies where the digital products themselves originate from another party or are owned by a person of another party. The provision does not apply to subsidies.	No less favourable treatment for like digital products from other jurisdictions. This applies where the digital products themselves originate from another party or are owned by a person of another party. Nothing prevents a Party from adopting or maintaining measures that limit the level of foreign capital participation in an enterprise engaged in the supply of broadcasting.	No less favourable treatment for like digital products from other jurisdictions. This applies where the digital products themselves originate from another party or are owned by a person of another party. The provision does not apply to subsidies and broadcasting.			N/A	
Domestic regulation	Binding commitment to maintain rules on electronic transmissions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996. Best endeavour commitments to facilitate stakeholder input in the development of those rules and avoid unnecessary regulatory burdens		Binding commitment to maintain rules on electronic transmissions 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. Best endeavour commitments to facilitate stakeholder input in the development of those rules and avoid unnecessary regulatory burdens			Each Party shall ensure that all its measures of general application affecting electronic commerce are administered in a reasonable, objective and impartial manner.	
E-signatures	Parties shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form. Parties shall encourage the use of interoperable electronic authentication	Parties shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.	Parties shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form. Parties shall encourage the use of interoperable electronic authentication	N/A	Parties shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form. Parties shall encourage the use of interoperable electronic authentication	Parties shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.	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. Parties shall encourage the use of interoperable electronic authentication and electronic signatures.
	Comment: Nearly all agreements include provisions for the acceptance of e-signatures. Those that go further encourage the interoperability of systems but make no formal commitments. The EU has historically adopted a more light touch approach to the acceptance of e- signatures, not often requiring firm commitments. However the recent EU-Japan EPA is in line with the more forward looking agreements. The CEPA goes further still by encouraging the use of interoperable electronic authentication and e-signatures.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Paperless trading	Each Party shall endeavour to accept a trade administration document submitted electronically as the legal equivalent of the paper version of that document	N/A	Each Party shall endeavour to make trade administration documents available to the public in electronic form; and accept trade administration documents submitted electronically as the legal equivalent of the paper version of those documents.	Each Party shall make publicly available, electronic versions of all existing publicly available trade administration documents. This is supplemented by active promotion of paperless trading through taking measures to make it simpler by having a single point of call to submit documentation, recognising the role of international standards and cooperation in international fora to enhance the acceptance of electronic versions of trade documents.	Each Party shall make publicly available, including through a process prescribed by that Party, electronic versions of all existing publicly available trade administration documents. This is supplemented by active promotion of paperless trading through taking measures to make it simpler by having a single point of call to submit documentation, recognising the role of international standards and cooperation in international fora to enhance the acceptance of electronic versions of trade documents.	N/A	
	Comment: USMCA and CPTPP include provisions that require soft commitments. DEPA and the SADEA push further to enhance and actively promote paperless trade. Indeed, the push towards including commitments, especially binding ones, on paperless trade has been driven traditionally by Australia and New Zealand. For the EU a provision on paperless trading is not found in most agreements. The US does not include this provision in all agreements but has done most recently.						
Online Consumer Protection	Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.	Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.	Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities.	Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities. Such laws may include general contract or negligence law and may be civil or criminal in nature. Each Party shall adopt or maintain laws or regulations that require, goods and services provided to be of acceptable and satisfactory quality, consistent with the supplier's claims and provide consumers with appropriate redress when they are not.	Each Party shall adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities. 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, such as the APEC Cross-Border Privacy Rules	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.	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. 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.
	Comment: The DEPA provides the current gold standard of what is achievable in online consumer protection. It reiterates the commitments made in the other trade agreements with stronger wording and more detail. Within EU FTAs the primary emphasis is usually on regulatory dialogue for consumer protection – so the wording of provisions is often softer. Although the CEPA goes beyond the EPA, it still falls short of the firmer commitments made in some of the other agreements which espouse the adoption or maintenance of a legal framework for consumer protection.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Unsolicited Commercial Electronic Communications	Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications. Each Party shall provide recourse in its law against suppliers of unsolicited commercial electronic communications that do not comply with this.	Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages. Suppliers of unsolicited commercial electronic should facilitate the ability of recipients to prevent ongoing reception of those messages; or require the consent. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained	Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that (a) require suppliers to facilitate the ability of recipients to prevent ongoing reception of those messages; (b) require the consent of recipients to receive commercial electronic messages; or (c) provide for the minimisation of unsolicited commercial electronic messages. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures	Reaffirms CPTPP	Reaffirms CPTPP	Each Party shall adopt or maintain measures regarding unsolicited maintain measures regarding unsolicited commercial electronic messages. Suppliers of unsolicited commercial electronic should facilitate the ability of recipients to prevent ongoing reception of those messages; or require the consent. Each Party shall ensure that commercial electronic messages are clearly identifiable as such. Each party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained.	Each Party shall adopt or maintain measures regarding unsolicited maintain measures regarding unsolicited commercial electronic messages. Suppliers of unsolicited commercial electronic should facilitate the ability of recipients to prevent ongoing reception of those messages; or require the consent. Each Party shall ensure that commercial electronic messages are clearly identifiable as such. Each party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained.
	Comment: CPTPP originally outlined the most binding commitments which have then been replicated in other trade agreements.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Protection of personal information	Parties 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 this legal framework, each Party should take into account principles and guidelines of relevant international bodies. Each Party shall publish information on the personal information protections it provides to users of digital trade. Each Party should encourage the development of mechanisms to promote compatibility between these different regimes.	Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. Each Party shall publish information on the personal information protections it provides to users of digital trade. Each Party should encourage the development of mechanisms to promote interoperability between these different regimes.	Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital tr ade. Each Party shall publish information on the personal information protections it provides to users of digital trade each Party should encourage the development of mechanisms to promote interoperability between these different regimes	As well as the provisions as outlined in CPTPP, DEPA provisions also state the Parties shall encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices. The Parties shall exchange information on and share experiences on the use of data protection trustmarks. The Parties shall endeavour to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information.	CPTPP provisions as well as a commitment to promote the CBPR System, with the aim to improving awareness of, and participation in, the CBPR System, including by industry.	N/A	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. Each Party shall publish information on the personal information protections it provides to users of electronic commerce. Each Party should encourage the development of mechanisms to promote compatibility between these different regimes.
	Comment: USMCA and SADEA align themselves with the APEC Cross Border Privacy Rules which include requirements for the protection of personal information of users of e-commerce and has among its aims the protection of the data of individual natural persons in e-commerce. The CBPR was first established in 2011 by the Asia-Pacific Economic Cooperation (APEC)—a "regional economic forum" of 21 Asian-Pacific member economies. Like the European Union's General Data Protection Regulation (GDPR), the CBPR also governs the transfer of personal information across the borders of participating countries. The DEPA goes further than the others by having slightly stronger wording on interoperability cooperation as well as provisions for trustmarks. Although this issue features prominently in policy debates in the EU, negotiators have not proactively sought such an obligation from their FTA partners. Provisions within CEPA have gone beyond those in the EU - Japan EPA and are on a par with the provisions within the USMCA and CPTPP.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Data flows	No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person. Covered person does not include a "financial institution" or a "cross- border financial service supplier of a Party". Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with the above that is necessary to achieve a legitimate public policy objective. From the Financial Services Chapter: No Party shall prevent a covered person from transferring information, including personal information, into and out of the Party's territory by electronic or other means when this activity is for the conduct of business within the scope of the license, authorisation, or registration of that covered person. Here a 'covered person' includes a financial institution or a cross-border financial service supplier of a Party.	Neither Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means, if this activity is for the conduct of the business of a covered person. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with the above that is necessary to achieve a legitimate public policy objective.	Each Party shall allow 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. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with the above that is necessary to achieve a legitimate public policy objective. Covered person does not include a "financial institution" or a "cross- border financial service supplier of a Party".	Reaffirms CPTPP commitments A Party may prevent or limit transfers by a financial institution or cross-border financial service supplier to, or for the benefit of, an affiliate of or person related to such institution or supplier, through the equitable, non-discriminatory and good faith application of measures relating to maintenance of the safety, soundness, integrity, or financial responsibility of financial institutions or cross-border financial service suppliers. This paragraph does not prejudice any other provision of this Agreement that permits a Party to restrict transfers.	Allows for the transfer of data between Australia and Singapore for business purposes, including in the financial sector.	Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement	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. Nothing in this Article shall prevent a Party from adopting or maintaining measures to achieve a legitimate public policy objective. 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.
	Comment: Some provisions related to data flows are contained within both the digital trade and financial services chapters in trade agreements. In USMCA for instance the provisions within the financial services chapter supplement and clarify those contained within the digital trade chapter. Within CPTPP, a covered person does not cover financial institutions. This has huge implications for financial services providers especially digital payment services necessary for online transactions. The DEPA allows parties to prevent or limit transfers by a financial institution for reasons relating to the safety, soundness, integrity, or financial responsibility of financial institutions or cross- border financial service suppliers. This however does not apply to electronic payments. Unsurprisingly, agreements with Singapore seem to the most forward looking. The SADEA includes financial data within data flows provision as does the CEPA which was seen as a welcome development by the UK FPS industry.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Data localisation	No 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. However, this is caveated with the provision that a country can adopt a localisation measure if it was needed to achieve a "legitimate public policy" 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 necessary to achieve the objective.	No 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. This Article does not apply with respect to covered financial service suppliers, which are addressed by Article 13.(below)	No 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. However, this is caveated with the provision that a country can adopt a localisation measure if it was needed to achieve a "legitimate public policy" 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 necessary to achieve the objective.	Reaffirms CPTPP	Reaffirms CPTPP commitments but does not apply to a "financial institution" or a "financial service supplier of a Party",	N/A	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. However, this is caveated with the provision that a country can adopt a localisation measure if it was needed to achieve a "legitimate public policy" 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.
	Comment: The USMCA, CPTPP, CEPA and DEPA text caveat the provisions with a carve out for legitimate public policy objectives. This is not contained within USMCA. US-Japan includes a specific provision for financial services which goes beyond USMCA. In contrast the SADEA carves out FS.The provision in CEPA is similar to that contained in the USMCA.						
Location of Financial Service Computing Facilities for Covered Financial Service Suppliers	N/A	Neither Party shall require a covered financial service supplier to use or locate financial service computing facilities in that Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on financial service computing facilities that the covered financial service supplier uses or locates outside the territory of the Party.	N/A	N/A	Neither Party shall require a covered financial service supplier to use or locate financial service computing facilities in the Party's territory as a condition for conducting business in that territory, provided that the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on financial service computing facilities that the covered financial service supplier uses or locates outside the Party's territory.	N/A	N/A
	Comment: The US - Japan Digital Trade Agreement and SADEA include an explicit provision prohibiting localisation for financial service suppliers.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Cooperation	The Parties shall endeavour to: (a) exchange information and share experiences on regulations, policies, enforcement and compliance; (b) cooperate and maintain a dialogue on the promotion and development of mechanisms, that forth global interoperability of privacy registered compliance; (c) participate actively in regional and multilateral fora to promote development of digital trade; (d)encourage development by the private sector of methods of self- regulation that foster digital trade; promote access for persons with disabilities to information and communications technologies; and (f) promote, through international cross-border cooperation initiatives, the development of mechanisms to assist users in submitting cross-border complaints regarding personal information protection. Parties shall consider establishing a forum to address the issues listed above or any other matter pertaining to the operation of the Chapter.	N/A	The Parties shall endeavour to: (a) work together to assist SMEs to overcome obstacles to its use; (b) exchange information and share experiences on regulations, policies, enforcement and compliance; (c) participate actively in regional and multilateral fora to promote the development of electronic commerce; and (d)encourage development by the private sector of methods of self- regulation that foster electronic commerce.	No dedicated chapter on cooperation but is included in several modules i.e. SMEs, cybersecurity competition policy and FinTech.	The Parties shall endeavour to: (a) exchange information and share experiences on regulations, policies, and enforcement and compliance mechanisms; (b) exchange information and share views on consumer access to products and services offered online between the Parties (c) exchange information on the development, reform, implementation and effectiveness of copyright legal frameworks relevant to the online environment; (d) exchange financial intelligence exchange financial intelligence and share capabilities to support regional efforts to counter terrorism financing, money laundering and other transnational organised crime (e) participate actively in regional and multilateral fora to promote the development of the digital economy and (f) encourage development by industry of methods of self-regulation that foster the digital economy Also covered by Articles on SMEs, cybersecurity, competition policy and FinTech and RegTech.	The Parties shall, where appropriate, cooperate and participate actively in multilateral fora to promote the development of electronic commerce. The parties agree to maintain a dialogue on regulatory matters relating to electronic commerce.	The Parties shall, where appropriate, cooperate and participate actively in multilateral fora to promote the development of electronic commerce. The Parties shall agree to maintain a dialogue on regulatory matters relating to electronic commerce.
	Comment: The emphasis on regulatory dialogue is contained within most provisions. In many trade agreements in the APAC region, there is a provision to facilitate the use of e commerce for SMEs. These trade agreements also initiated an emphasis on the importance of governments collaborating with the private sector to develop initiatives to govern cross border electronic transactions.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Cybersecurity	The Parties shall endeavour to (a) build the capabilities responsible for incident response; and (b) strengthen existing collaboration to encourage enterprises to use risk-based approaches that rely on consensus-based standards to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.	Same as USMCA	The Parties recognise the importance of building the capabilities of their national entities responsible for security and incident response; and using existing collaboration mechanisms to identify and mitigate malicious intrusions that affect the electronic networks of the Parties.	The Parties have a shared vision to promote secure digital trade to achieve global prosperity and recognise that cybersecurity underpins the digital economy The Parties recognise the importance of building the capabilities responsible for security and incidence response. Commit to using existing collaboration mechanisms to cooperate on workforce development in the area of cybersecurity, including through possible initiatives relating to MRPQs, diversity and equality.	Same as in DEPA	Maintain a dialogue on cybersecurity	Maintain a dialogue on cybersecurity
	Comment: The EU - Japan EPA has a light touch approach here. DEPA and the SADEA are more comprehensive insofar as they recognise the importance of workforce development in this area.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
Source code	No Party shall require the transfer of, a source code of software owned by a person of another Party, or 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. This does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code for a specific investigation, examination or judicial proceeding.	Neither Party shall 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. This does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code for a specific investigation, examination or judicial proceeding.	No Party shall require the transfer of a source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory. This provision is limited to mass-market software or products containing such software and does not include software used for critical infrastructure. This does not preclude the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts or a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.	N/A. Only includes provisions for the protection of encryption. The Parties affirm their level of commitments relating to Information and Communication Technology products that use cryptography.	Neither Party shall require the transfer of a source code of software. This does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve or make available the source code of software to the Relevant Body for a specific investigation, examination or judicial proceeding. This does not preclude the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts or a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement If both Parties undertake obligations not require the transfer of, or access to, an algorithm expressed in source code of software owned by a person of a Party or non-Party as a condition for the import, distribution, sale or use of that software, or of products containing that software, in their respective territories, this Article shall apply, mutatis mutandis, to algorithms expressed in source code of software owned by a person of the other Party.	A Party may not require the transfer of, source code of software owned by a person of the other Party. Nothing in this paragraph shall prevent the inclusion or implementation of terms and conditions related to the transfer of or granting of access to source code in commercially negotiated contracts, or the voluntary transfer of or granting of access to source code for instance in the context of government procurement.	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. This does not preclude a regulatory body or judicial authority from requiring a person of the other Party to (q) preserve and make available the source code of software, or an algorithm expressed in that source code for a specific investigation, examination or judicial proceeding 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.
	Comment: USMCA, like CPTPP, stipulates that governments cannot force companies to the disclose source code in order to enter a market . USMCA, CEPA, SADEA, UK – Japan Digital Trade Agreement go a step further and extend this protection to algorithms. CPTPP is limited to mass-market software and does not include critical infrastructure.						

	USMCA	US-Japan Digital Trade Agreement	CPTPP	DEPA	SADEA	EU - Japan EPA*	CEPA*
SMEs	N/A	N/A	N/A	Module 10 on SME cooperation. The Parties shall foster close cooperation on the digital economy between SMEs of the Parties and cooperate in promoting jobs and growth for SMEs Additional commitments on (a) cooperation to enhance trade and investment opportunities for SMEs; (b) information sharing and (c) convening a Digital SME Dialogue.	The Parties shall endeavour to: (a) exchange information and best practices in leveraging digital tools; (b) cooperate in other areas that could help SMEs; (c) encourage participation by SMEs in online platforms and other mechanisms that could help SMEs link with international business partners and (d) foster close cooperation on the digital economy between SMEs of the Parties.	N/A	N/A
	Comment: All of the trade agreements make mention of SMEs and helping to facilitate their use of ecommerce. DEPA, EU - Japan and SADEA include specific chapters/modules on SMEs with EU-Japan providing a one point 'helpdesk' for SMEs and DEPA committing to convening an Digital SME Dialogue.						
Open Government Data	To the extent that a Party chooses to make government information, including data, 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. The Parties shall endeavour to cooperate to identify ways in which each Party can expand access to and use of government information, including data, that the Party h as made public, with a view to enhancing and generating business opportunities, especially for SMEs.	Same as USMCA	N/A	Same as USMCA but no specific mention of SMEs. Examples of cooperation given are jointly identifying sectors where open data sets, can be used to facilitate technology transfer, talent formation and innovation; encouraging the development of new products and services based on open data sets and fostering the use and develop open data licensing models in the form of standardised public licences available online, which will allow open data to be freely accessed, used, modified and shared by anyone	To the extent that a Party chooses to make government information available to the public, it shall endeavour to ensure: that the information is appropriately anonymised, contains descriptive metadata and is in a machine readable and open format that allows it to be searched, retrieved, used, reused and redistributed; and to the extent practicable, that the information is made available in a spatially enabled format with reliable, easy to use and freely available APIs and is regularly updated. 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 and research opportunities.	N/A	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. 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 SMEs.
	Comment: Access to open government data is a relatively new provision which goes hand in hand with the development of AI as access to large data sources are crucial to train AI programs. USMCA has set a gold standard that commits parties to make government data available to the public in machine-readable and searchable open formats, and allow it to be searched, retrieved, used, reused, and redistributed. This is replicated in DEPA and the SADEA.						

Acknowledgements

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.

Contributors to the Report

Tehreem Yusuf
Global Trade Policy Adviser
+44 (0) 7841 533719
tehreem.yusuf@cityoflondon.gov.uk

Alexandra Mills
Senior Global Trade Policy Adviser
+44 (0) 7544 656861
alexandra.mills@cityoflondon.gov.uk

Duncan Richardson
Head of Global Trade Policy
+44 (0) 7841 514872
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.

CITY OF LONDON

cityoflondon.gov.uk