frontier economics

THE EXTENT AND IMPACT OF DATA LOCALISATION

Report prepared for DCMS

1 June 2022

CONTENTS

EXECUTIVE SUMMARY

Definitions of "data localisation" vary, and reflect the complex interplay of factors that motivate jurisdictions to restrain or impose conditions on cross-border data flows

"Data localisation" is a complex phenomenon, not least because there is no settled definition of the expression. For the purposes of this research, we consider data localisation to refer to the extent to which data that are generated in a jurisdiction (e.g. by businesses, organisations or individuals) are subject to legal and administrative measures that restrict the use of those data outside that jurisdiction. These restrictions include requirements that data need to be stored in facilities within the jurisdiction, and that there are restrictions on the accessing, transmission or processing of data on a cross-border basis. Restrictions may be absolute, in the sense that no cross-border transmission of data is allowed, or conditional, in the sense that they permit cross-border transmission provided certain conditions are met.

The complexity of the definition reflects the different forces at play in shaping data governance frameworks, and the attempts by authorities to strike a balance between them. Specifically, while governments tend on the whole to recognise the facilitating role that cross-border data flows can play in regard to trade and investment, they also typically seek to pursue a range of public policy objectives. These include privacy of personal data, national security, dealing with market power, sectoral regulation matters, and industrial policy. Pursuing these objectives can lead authorities to limit, or impose conditions on, cross-border data flows. That in turn suggests there may be trade-offs between the pursuit of these wider public policy objectives, on one hand, and the specific benefits that could be associated with liberalising cross-border data flows. Jurisdictions vary in how they handle these concerns and in the trade-offs between them. Approaches to managing these trade-offs can reflect national, or regional, sensitivities and attitudes to risk, and legal and political arrangements. This in turn results in a complex international data localisation (and data governance) landscape.

The international landscape for data localisation is complex, with trends towards more restrictiveness in certain jurisdictions

Comparative assessments of data localisation are challenging, but one way of making such assessments is by considering how restrictive policies are. We reviewed the policies of 45 jurisdictions. Of these, China, India and Vietnam have the most restrictive policy settings. In the case of China, a patchwork of laws appears to carry a clear implication: data localisation is the default, cross-border transfers are the exception. Russia can also be considered more restrictive due to its cross-cutting requirement that a copy of all personal data be stored locally.

Some jurisdictions use a "positive" or "white" list approach to enable transfers of personal data. Such approaches typically specify conditions that partner jurisdictions need to satisfy, and, if they do, allow for cross-border personal data flows without the need for additional safeguards. We say "positive" or "white" list since the default is not liberalisation: only if there is a specific determination that conditions are met can liberalisation take place. The EU General Data Protection Regulation (GDPR) is an example of this. It requires an extensive process to determine whether the partner's data regime is essentially equivalent. Other jurisdictions that follow a similar white list approach are, for example, Switzerland and Japan. In the absence of a positive determination, the policy settings may be more restrictive for the transfer of personal data. This typically does not mean that cross-border personal data flows cease: there may be other measures and instruments that businesses and organisations that businesses may be able to put into place to facilitate transfers. For example, binding and enforceable

internal rules and policies for data transfers within multinational group companies, or standardised data protection contractual clauses. The point, however, is that these case-by-case measures are likely to involve greater transaction costs than a broad authorisation for data transfer, and therefore represent a lower degree of cross-border data flow liberalisation. Some jurisdictions make cross-border personal data flows conditional on obligations of conduct that apply to the user or processor of data (rather than making a determination about partner country regime). These include seeking informed consent and implementing reasonable safeguards prior to data transfer. Jurisdictions which follow this approach include Australia, Canada, Singapore and New Zealand. These jurisdictions, along with the USA, have the lowest level of data localisation requirements.

International trade agreements can help to lock in existing levels of liberalisation, create more transparency and predictability in relation to policy affecting cross-border data flows, and promote further liberalisation

Data provisions can be found in preferential free trade agreements (both bilateral or regional), as well as in bespoke data or digital agreements, including pluri-lateral initiatives. These agreements can play a significant role in disciplining the extent of data localisation a country may pursue. By "disciplining", we mean several related effects:

- Commitments to eliminating or not imposing restrictions on cross-border data flows. If countries already impose low levels of restrictions, these commitments can limit the extent to which they may roll back existing levels of liberalisation and impose new restrictions, thus helping to promote a liberal environment for data flows and trade.
- Trade agreements allow for the possibility of imposing restrictions on cross-border data flows to pursue wider public policy goals. But they usually try to limit the scope for discretionary restrictions by requiring that such measures taken are necessary to achieve the stated aim and are not a disguised restriction on trade or unjustified discrimination.

The strength of the trade agreements in terms of their disciplining effects can vary considerably. The US-Mexico-Canada Agreement (USMCA) has, on paper at least, the strongest disciplines. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) contains substantial data provisions as well, although the scope for discretionary intervention is potentially wider than in the USMCA. The UK-Japan and UK-EU agreements also contain substantial disciplines, the latter goes further than those typically negotiated by the EU.

Restrictions on cross-border data flows impose costs on international trade. Measuring the effects of these trade costs is a way of understanding the transnational impact of data localisation policies. The links between trade and economic growth also help us to estimate the impact of data localisation at the national level. We infer effects on economic growth by using measures of the responsiveness of gross value added (GVA) (a measure of the value of goods and services produced by a sector or economy) to changes in trade, a methodology used notably by HM Treasury in its analysis of the long-run impacts of the UK leaving the EU.

Cross border data flows play a significant role in stimulating trade. Like many major economies, the UK would face adverse impacts from an upswing in restrictiveness on cross-border data flows

We model the effects of data localisation on seven countries – China, India, France Japan, Mexico, South Korea and the USA – and on the EU. The selection of countries reflects UK trade patterns and policy priorities across different levels of development. We also model results for the UK, as part of a broader analysis of the effects of data localisation on the UK (see relevant subsection below)

There are many ways in which the effects of localisation can be measured. We chose the following approach:

- We model a worst scenario in which the countries and their trade partners move from current policy settings to a high level of restrictiveness on cross-border data flows. In practice, this means that local data storage is mandated and that the transfer of data for storage overseas is prohibited. This reflects recent trends favouring greater restrictions. It is also a way of measuring the costs that could be avoided via provisions in trade agreements (including FTAs) that lock-in existing liberalisation or reduce the possibility of roll-back.
- Secondly, beginning with the fully restricted settings described in the first scenario above, we project a hypothetical scenario in which the countries of interest and the EU agree on reciprocal arrangements that allow the bilateral free flow of data, including for personal data via an adequacy determination made by the EU. The scenario also reflects the fact that UK operates a level of standards based on the EU GDPR. The reduction in losses (i.e. the difference in the absolute value of losses) between the first and the second scenario represents the value of reducing barriers through the forms of arrangements described above.

The results are presented in the table below.

Figure 1 Summary of country-level trade and GVA impacts

Country	Trade impacts Scenario 1	Trade impacts Scenario 2	GVA impacts Scenario 1	GVA impacts Scenario 2
UK	-8.6%	-4.6%	-2.3%	-1.2%
China	-3.6%	-2.7%	-0.9%	-0.7%
India	-7.1%	-5.9%	-1.8%	-1.5%
Japan	-7.3%	-6.4%	-1.8%	-1.6%
South Korea	-6.5%	-5.8%	-1.6%	-1.5%
Mexico	-8.1%	-7.9%	-2.0%	-2.0%
US	-8.8%	-6.9%	-2.2%	-1.7%
France	-7.1%	-3.8%	-1.8%	-0.9%
EU	-6.7%	NA	-1.7%	NA

Source: Frontier calculations based on OECD data.
Note: Scenario 2 is not applicable to the EU.

The results for scenario 1 underscore the exposure of the countries to data restrictions The losses on trade reflect the fact that data restrictions act as an implicit tax on sectors that use data intensively as part of their operations. Given that most FTA commitments have the effect of locking-in existing levels of liberalisation, the results highlight the costs that can be avoided through such locking-in effects. These measures of avoided costs could understate the benefits of locking-in. This is because locking-in removes, to some extent, uncertainty to businesses, which in turn can facilitate investment decisions.

Both trade effects and GVA effects represent annual losses that are incurred each year. The GVA effects are computed on the basis of a measure of the responsiveness ("elasticity") of changes to GDP in relation to changes in trade (an approach followed by HMT Treasury in its calculation, for example, of the long run effects of the UK leaving the EU). The greater the changes in exports, the bigger the change in GVA.

Under scenario 2, reported losses fall because countries move from high restrictions to reciprocal arrangements for liberalised bilateral cross-border data flows with the EU,.

Understandably, the reduction in losses are highest for countries which have the highest trade exposure to the EU. For all countries, the reduction in losses relative to scenario 1 measures the avoided costs of measures affecting cross-border data flows with the EU.

High restrictions on bilateral data flows to non-EU jurisdictions mean that a large proportion of the costs incurred under the high restrictions scenario still persists. For countries with less trade exposure to the EU, the results suggest that their main priority should be to pursue rules that help to secure bilateral cross-border data flows with non-EU countries by, at the very least, locking in current levels of liberalisation.

China is an outlier in that the results are relatively muted. The reason for this is that data flows between China and the rest of the world are already highly restricted, so incremental losses under scenario 1 are limited. Given this situation, we model an extra scenario for China, in which it brings its own restrictions to levels commensurate with the average for the rest of the world. This unilateral liberalisation (i.e. undertaken without any liberalisation on the part of partners) would add close to 2.5% to China's exports or around 0.6% to GVA.

In addition to the overall effects, we can identify the following sectoral patterns.

Certain commonalities can be observed across countries:

- The highest absolute effects are observed in high-value manufacturing,[1] reflecting the size of these sectors in trade and the importance of data to the operation of these sectors. The exception is India, where the effects of data localisation on information technology (IT) services are greater.
- The introduction by a country of restrictions on cross-border data flows has a significant effects on its own exports, that usually dominates the effects of a partner's measures, i.e. data localisation is a tax on a country's exports. This is borne out by the additional scenario we model for China. One of the implications is that relaxing one's own localisation restrictions will have a bigger export-boosting effect than measures taken by partners.
- The "export tax" effect of data localisation is in line with the observed effect of trade restrictions generally on export behaviour. In this particular case, data localisation imposes costs, both in the form of compliance costs and higher input costs, on domestic data-intensive industries. Cost increases can also raise the height of barriers to entry in these industries. That effect provides an advantage to incumbent businesses who can find supplying the more sheltered domestic market more attractive.
- In proportionate terms, services sectors tend to be more heavily impacted. This reflects their high degree of data dependency, notably in publishing, IT and telecoms, financial and business services. For some countries, negative impacts are between a fifth and a quarter of sector exports. Absolute values are also high in certain cases, notably:
  - Financial services in the USA
  - Business services in the USA and the EU
  - IT and computer services in India.

The modelled effects underscore the value of data provisions in international trade agreements. In particular, the way in which the scenarios are specified underscores the importance of trade agreements in locking-in existing levels of liberalisation, and therefore avoiding the costs associated with an upsurge in localisation. Moreover, as a substantial proportion of these adverse effects are generated by one's own data localisation measures,

[1] Defined as goods sectors excluding agriculture and primary commodities, food manufacturing, and textiles and clothing.

trade agreements act as a discipline on a country's own policy: they provide a measure of security for sectors that depend on data flows in the face of domestic pressures to restrict such flows.

All the selected economies, with the exception of China (which is already highly restrictive in its approach to cross-border data flows), stand to suffer economic losses from increased restrictions on cross-border data flows. A key finding is that a country's own data localisation measures have a bigger impact on its own exports than measures taken by partners; data localisation acts as a tax on a country's own exports.

It is possible that the reported GVA impacts understate the true costs of restrictions on cross-border data flows. This is because data restrictions may have effects on innovation in nascent activities such as artificial intelligence that in turn can have positive effects on productivity over time. Such productivity enhancing effects, stemming from effects that are likely to materialise over time, are (at best) imperfectly captured by the quantitative framework we have employed.

The results underscore the value of international collaboration in maintaining a low level of restrictions on cross-border data flows, and finding ways to ensure that wider public policy objectives are pursued through means that are no more restrictive on trade than necessary.

Within the UK, London and the South East are the most exposed

The modelling for the UK extends the modelling done for other countries in a number of ways. In particular:

- We model an extra hypothetical scenario in which, starting from a high level of cross-border data restrictions, the UK concludes a FTA with the USA and Mexico with data provisions along USMCA lines, and joins the CPTPP. It does not enter into reciprocal arrangements with the EU (a position modelled under scenario 2).
- We present regional and firm-level results based on this modelling.

The trade results for the UK as a whole and by region are reported in the table in Figure 2.

Figure 2 Trade impacts by region (%)

	Scenario 1	Scenario 2	Scenario 3
North East	-7.7%	-3.5%	-5.6%
North West	-7.9%	-4.9%	-5.2%
Yorkshire and The Humber	-6.5%	-3.3%	-4.5%
East Midlands	-8.4%	-4.8%	-5.7%
West Midlands	-8.1%	-5.1%	-5.2%
East of England	-7.8%	-4.7%	-5.2%
London	-10.7%	-5.2%	-7.6%
South East	-8.9%	-4.7%	-6.3%
South West	-8.0%	-4.6%	-5.3%
Wales	-6.1%	-2.7%	-4.5%
Scotland	-6.1%	-3.6%	-4.0%
Northern Ireland	-8.2%	-4.5%	-5.7%
UK total	**-8.6%**	**-4.6%**	**-5.9%**

The impacts of scenario 1 (full restrictiveness) on London stand out, mainly because of the concentration of data-intensive services sectors.

The reduction in losses between scenario 1 and scenario 2 represent the effects on regions of reciprocal bilateral arrangements with the EU (including an adequacy determination by the latter) that preserve existing levels of cross-border data liberalisation. London, the North East and Wales are the biggest beneficiaries, and the gains for all regions are relatively substantial.

The difference between scenario 1 and scenario 3 is the latter captures the effects of the UK pursuing agreements with the US, Mexico and CPTPP countries, and thereby securing existing levels of liberalisation with these countries. The differences are substantial but are generally smaller than those associated with the differences between scenario 1 and scenario 2.

For GVA impacts at the regional level, we undertake a bottom-up analysis which adopts the approach recommended by the HM Treasury Green Book (i.e. the official UK government resource that sets guidelines for impact and project evaluation) and assume that rather than outright job losses, workers instead move into less productive jobs. This is different to the approach used to infer GVA effects reported in Figure 1 and yields more moderate GVA effects. These are reported in Figure 3.

Figure 3 GVA impacts by region (%)

	Scenario 1	Scenario 2	Scenario 3
North East	-0.6%	-0.3%	-0.4%
North West	-0.4%	-0.2%	-0.3%
Yorkshire and The Humber	-0.4%	-0.2%	-0.2%
East Midlands	-0.4%	-0.3%	-0.3%
West Midlands	-0.6%	-0.4%	-0.4%
East of England	-0.4%	-0.2%	-0.3%
London	-0.9%	-0.5%	-0.6%
South East	-0.5%	-0.3%	-0.4%
South West	-0.4%	-0.2%	-0.3%
Wales	-0.5%	-0.2%	-0.3%
Scotland	-0.5%	-0.3%	-0.3%
Northern Ireland	-0.3%	-0.2%	-0.2%
UK total	-0.6%	-0.3%	-0.4%

The numbers for the UK as a whole are lower than those reported in Figure 1 because of differences in methodology. The approach underpinning the results in Figure 1 allows for a wider range of effects through productivity spillovers across sectors and does not assume full employment.

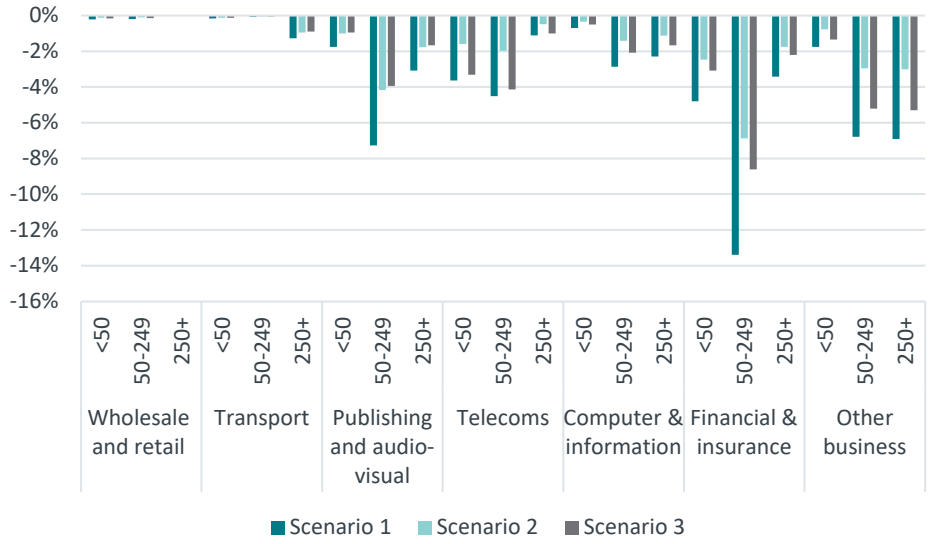
The results show a considerable degree of variation across the UK, in line with each region's exposure to trade in goods and services that are data intensive.

If applied to the UK as a whole, the results across the three scenarios yield GVA effects of -2.2%, -1.2% and -1.6% respectively. Put together, the results in Figure 3 can be considered a lower bound, in absolute value terms, while the results based on the methodology underpinning Figure 1 can be considered an upper bound.

We also examine the impacts of these scenarios on businesses in relation to their size. To do this we use the Office for National Statistics (ONS) International Trade in Services (ITIS) microdata. There is some variation across sectors in the extent to which businesses of different sizes rely on exports (as represented by the share of exports in turnover). We

therefore report the impact of the three scenarios in terms of export impacts as a proportion of turnover (Figure 4).

Figure 4 Trade impacts as a proportion of firm turnover, by sector, size band and scenario



The differences between sectors reflect their sensitivity to data flows, as defined in the Services Trade Restrictiveness Index (STRI), as well as the specific changes modelled in the scenarios. Within a given sector, the relative impact by size band reflects its exposure in terms of exports as a proportion of overall turnover. The strongest impacts as a percentage of turnover are seen in the publishing/audio-visual and financial/insurance sectors, particularly in the 50-249 employee size band.

Qualitative evidence suggests significant gaps in understanding and preparedness by businesses concerning data localisation requirements

We supplemented the quantitative analysis with a qualitative analysis. This was based on a YouGov survey of 2,000 businesses supplemented by in-depth interviews.

The results of the YouGov business survey revealed a level of discordance between the majority of respondents, on one hand, who agreed that high levels of data localisation would adversely affect them, while, on the other, a large majority professed to be unaware of the nature of data requirements in the countries to which they exported. Unawareness does not appear to be a function of business size: it is an issue for large and small firms.

This could leave businesses vulnerable to sudden changes in government action, especially enforcement, in specific countries. Such changes in legislation around cross-border data flows in countries of export could leave businesses exposed, resulting in a significant negative impact for these businesses. The impact would be particularly strong on smaller businesses which typically lack the capacity and resources to invest in bespoke compliance solutions.

This highlights the value of transparency in measures across key countries of export for British businesses and the importance of businesses ensuring they have a solid understanding of the data requirements in place in countries they are operating in. Overall, to enable this, this may suggest there is value in seeking data provisions in trade agreements to provide more predictability and transparency.

Going forward, it may be helpful to undertake further research to understand the nature and magnitude of any negative impacts businesses may expect to deal with if faced with more restrictive data requirements in countries of export, and any measures businesses may already have in place to mitigate this.

The businesses that took part in the interviews were self-selecting and, therefore, any comparison between their views and those of surveyed firms is necessarily hazardous. Interviewed firms tended to show a high level of awareness and agreed that data restrictions introduced a range of costs to businesses and to consumers. They identified China, India Russia and Vietnam as countries in which data localisation was particularly problematic. In regard to the EU, their position tended to be that while the GDPR posed various challenges in terms of compliance, it was likely to emerge as a global standard and that, therefore, investing resources in compliance was worthwhile.

The majority of the businesses which export goods and/or services to the listed countries stated that they would be negatively impacted if the countries that they operate in required that all data from clients and employees in those countries had to be stored exclusively in those countries.

Read in conjunction with the survey results, the interviews suggest a certain sorting between businesses and, specifically, those that are data aware and those that are data unaware, and that substantial numbers of the latter exist across all sectors. The existence of a likely sizeable bloc of data-unaware businesses could mean that the modelled costs of data localisation – which primarily pick up trade costs – might understate the true costs of localisation.

1 INTRODUCTION

1.1 Context and objectives of this report

Frontier Economics has been commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to undertake a study into the extent and impacts of data localisation measures implemented internationally. By data localisation, we mean the extent to which data that are generated in a jurisdiction (e.g. by businesses, organisations or individuals) are subject to measures that restrict the use of those data outside that jurisdiction. These restrictions include requirements that data need to be stored in facilities within the jurisdiction, and that there are restrictions on the accessing, transmission or processing of data on a cross-border basis. Restrictions may be absolute, in the sense that no cross-border transmission of data is allowed, or conditional, in the sense that they permit cross-border transmission subject to certain conditions.

The interest in data flows and measures that affect them stems from their centrality to the economic activity of modern economies, notably in economies such as the UK in which services and high value-added manufacturing activities play an important role. Recent analyses have, for example, identified the emergence of data-enhanced businesses and data-intensive businesses.[2]

Data-enhanced businesses are ones whose operational models have gained in efficiency because of data flows. These efficiencies can be organisational in nature, e.g. the ability to develop cross-border value chains that in turn exploit gains from the specialisation of production in different locations, reflecting their cost advantages. Alternatively, they can reflect the ability to enhance products by improving functionality and performance (e.g. the integration of software services into automotive manufacturing).

Data-enabled businesses are ones whose core business model involves the use of data – whether in terms of storage or processing. These include platform and network service providers, analytics businesses and so forth. The distinction between these and data-enhanced businesses is obviously not watertight; many businesses may straddle both categories.

While the role played by data in modern commercial operations suggests reasons for liberalising cross-border data flows, jurisdictions also implement measures that restrict or regulate such flows. These measures may reflect a number of objectives, including public policy objectives relating to the safeguarding of privacy; security; regulatory objectives (e.g. prudential regulation in financial services); and industrial policy objectives relating to home-grown data infrastructure and capability.

Faced with this context, the UK is developing its approach to data governance and has already agreed provisions on data in the bilateral trade agreements that it has negotiated.

1.2 Objectives of the report

Given this context, the report is structured as follows:

[2] David Nguyen and Marta Paczos (2020), "Measuring the economic value of data and cross-border data flows, A business perspective", OECD Digital Economy Papers, No. 297.

- Section 2 examines the extent of data localisation internationally, by presenting:
  - A cross-country panorama of measures addressing cross border data flows
  - An overview of how data flows and restrictions on these are addressed in trade agreements
- Section 3 presents deep dives into the nature and impacts of data localisation policies in China, France, India, Japan, South Korea, Mexico, the USA and the EU. This includes economic modelling of the impacts of data localisation measures via the effects these measures have on international trade.
- Section 4 presents the impact of data localisation measures on the UK. The results are presented on an economy-wide basis and are also disaggregated on a regional basis and by business size.
- Section 5 presents the results of our qualitative analysis, based on survey results and interviews with individual stakeholders.
- Section 6 presents some concluding observations.

2 THE EXTENT OF INTERNATIONAL DATA LOCALISATION

2.1 A cross-country panorama

There is no commonly accepted definition of data localisation. As already observed in section 1.1, the concept of data localisation can cover a number of different measures and can be implemented in a number of different ways. For the purposes of this report, we adopt a broad view and consider data localisation measures to include:

- Mandatory legal requirements that are associated with penalties or sanctions in the event of non-compliance;
- Rules related to data storage, accessing or processing. Data storage refers to the physical systems (servers and related hardware) in which data and sets of data are stored. Data access refers to the ability to retrieve and use data that are so stored. Data processing refers to operations performed on data to develop new information; and
- Absolute and conditional measures. Absolute measures impose restrictions at all times. Conditional measures impose restrictions when certain factors apply. A common requirement is that cross-border data flows are permissible on condition that the destination jurisdiction has similar arrangements for data protection) or demonstrates that it meets certain minimal criteria, or that the business transferring data satisfies certain obligations of conduct.

The actual impact of restrictions on cross-border data flows depends on a number of factors. The overall stringency of the requirements is clearly a key factor. In principle, the dimensions presented above could be used as a guide to stringency. For example, the broader the scope of the requirements (storage, access and processing) and the more the requirement tends towards absolute requirements, the greater the level of stringency.

However, the relationship between these different dimensions and stringency is not straightforward. For example, the requirement to keep a copy of data on local servers (as is the case in Russia, see below) is an absolute requirement that does not preclude cross-border data flows, but likely adds to the transaction costs of businesses. On the other hand, a conditional requirement which predicates data flows on a criterion of equivalence (as is the case with the GDPR and the requirement for adequacy, for example) can also entail significant restrictions on personal data flows when equivalence is not met. The practical effects on businesses may not be different from absolute requirements, depending on the nature of the business.

The last point highlights the fact that, beyond the question of stringency, a key question is the impact on transaction costs at the firm level. Stringency is a driver of transaction costs to businesses through resources devoted to compliance and, potentially, changes to business operations. Sections 3 and 4 draw on the concept of transaction costs to model the effects of varying stringency in data localisation on trade, while sections 5.2 and 5.3 report the views of businesses on the effects of requirements on business operations via transaction costs.

In the remainder of this section, we present an overview of data localisation requirements globally by using the different concepts described above to analyse laws and regulations across a range of major economies. This cross-country panorama is presented in the table in

Figure 5 at the end of this section. The table assesses localisation requirements using the dimensions described above.

The main trends that emerge are as follows:

- Formal absolute localisation requirements are relatively rare. Those that apply on an economy-wide basis often apply to specific functions. For example, in several EU member states, such as Belgium, Germany, Denmark and Finland, accounting and invoicing data need to be stored locally, though this does not preclude storage outside the country. Similar requirements are found in New Zealand. Sector-specific absolute localisation requirements are more prevalent in relation to public sector data (typically fiscal and health data) and the financial sector, where regulators often require local storage to facilitate access for prudential reasons.
- The strongest formal absolute economy-wide restrictions are found in Vietnam, India and, to a lesser extent, Russia. In Vietnam, all locally generated data must be held locally. In India, critical personal data are not allowed to be stored outside the country under the draft Data Protection Bill. Ambiguity regarding what comes under the scope of critical personal data, and difficulties in segmenting between these and other data, creates both complexity and compliance. Moreover, this distinction does not necessarily correspond to how businesses, and particular data-enabled ones like platform services, segment data. If that is the case, the reach of the prohibition may, in practice, extend to all forms of data (see also section 3.4).
- The picture on data localisation is clouded by the fact that even if countries do not have formal absolute requirements, the practical impact of the way data governance is implemented curtails the cross-border flow of data. This is notably the case with China. On paper, cross-border data flows are not prohibited, but there is no automaticity in data transfer or a set process for mutual recognition with partners that would facilitate such transfer. Indeed, the general presumption is that data flows from China are not possible, and assessments of Chinese policy set its level of restrictiveness as amongst the highest in the world. Indeed, some businesses (see section 5.3) consider China's data regime, and digital landscape more generally, to operate separately to the rest of the world. In the case of Malaysia, cross-border flows are permissible to countries on a white list, but there is, to date, a lack of clarity as to the coverage of this list.
- Approaches vary across countries that implement conditional localisation (or by the same token, allow cross-border flows subject to conditions being met). The GDPR is an example of a positive list approach – it provides for free flows of personal data with countries which are deemed to provide adequate data protection and which the EU has thus selected for inclusion on a list of countries. The EU sets a high bar for inclusion on this list, not least being assessed as having data protection standards that are essentially equivalent to the EU's; and only a small number of countries have acquired this status. For countries not on this list, transfers are possible, in principle, subject to standard contractual clauses or binding corporate rules that safeguard the principles of the GDPR (though, as discussed in section 3.9.2, recent European Court of Justice (ECJ) rulings in the Schrems II case have fragilised this approach). Other jurisdictions that follow this approach include Switzerland and Japan. Data governance frameworks followed in Argentina and Brazil are also deemed to follow similar approaches.
- Other approaches to conditional localisation involve the authorisation of cross-border flows subject to the data user or processor satisfying obligations of conduct. These include seeking informed consent and implementing reasonable safeguards. Jurisdictions which

follow this approach include Australia, Canada, Singapore and New Zealand. These jurisdictions, along with the USA, have the lowest level of localisation requirements.

- The UK implemented the GDPR, which it inherited from its membership of the EU. It is currently determining the future shape of its data policy, with some indications via its National Data Strategy that it considers the GDPR approach, notably in relation to adequacy, to be potentially too restrictive on cross-border personal data flows vis-à-vis the rest of the world. As documented in section 4, one question it may have to address is the extent to which pursuing a more liberal approach to cross-border data globally may increase frictions on data flows between it and the EU.

Beyond the snapshot provided by the panorama, it is useful to comment on underlying trends. In general, there is a recognition that the international landscape for data governance and data localisation specifically has become more complex.[3] This is due to the interplay of a number of factors, including a multiplicity of public policy objectives (such as privacy, security, addressing market power of digital platforms), industrial policy and the desire to facilitate trade through cross-border data flows. On this last subject, it should be noted that the absence of any rules on data may not necessarily facilitate cross-border flows. That is because parties may be not be willing to transfer data precisely because they do not think there are sufficient safeguards.

From an economic perspective, what matters is how these various objectives are balanced and the trade-offs between them are addressed. This arbitration happens at a domestic level but is also the subject of international negotiations, including in the context of trade agreements. This issue is the focus of section 2.2. The interplay between international arrangements and national ones is important as it can: (i) provide disciplines which limit the scope for discretionary changes that hinder cross-border data flows in a manner that is not proportionate to achieving policy objectives, and (ii) provide mechanisms to address the emerging complexity of the international data landscape by providing mechanisms for harmonisation and mutual recognition that in turn facilitate cross-border data flows and, by extension, trade.

[3] See for example, Dan Svantesson (2020), “Data localisation trends and challenges”, OECD Digital Economy Papers, No. 301.

Figure 5 Summary of data localisation measures

Country	Data can be transferred to countries offering "comparable" protection	Economy-wide requirements for local storage of data (but not local processing of or local access to data)	Economy-wide requirements for local storage of, processing of and access to data	Sector-specific requirements for local storage of data (but not local processing of or local access to data)	Sector-specific requirements for local storage of, processing of and access to data	Measures relate to personal data	Measures relate to other types of data
Argentina	Yes	No	No	No	No	No	No
Australia	Yes	No	No	Yes	Yes - for health data	Yes	No
Austria	Yes	No	No	No	No	No	No
Belgium	Yes	Yes – accounting records and invoices	No	No	No	No	Yes
Brazil	Yes	No	No	Yes – for the financial services sector and public sector	Yes - for the financial services sector and the public sector	Yes	Yes
Bulgaria	Yes	No	No	Yes - for the gambling sector	No	Yes	Yes
Canada	Yes	No	No	Yes - for public sector data	Yes - for public sector data	Yes	Yes
China	No	No	Yes - personal data and "important business" must be stored, processed and accessed in China unless a security assessment is passed	Yes - for financial services sector data, health data, mapping data, taxi/ride-sharing data	Yes - for financial services sector data, health data, mapping data, taxi/ ride-sharing data	Yes	Yes
Croatia	Yes	No	No	No	No	No	No
Cyprus	Yes	No	No	No	No	No	No
Czech Republic	Yes	No	No	No	No	No	No
Denmark	Yes	Yes - for accounting records	No	Yes - for public sector accounting records	No	No	Yes
Estonia	Yes	No	No	No	No	No	No
Finland	Yes	Yes - for accounting records	No	No	No	No	Yes

Country	Data can be transferred to countries offering "comparable" protection	Economy-wide requirements for local storage of data (but not local processing of or local access to data)	Economy-wide requirements for local storage of, processing of and access to data	Sector-specific requirements for local storage of data (but not local processing of or local access to data)	Sector-specific requirements for local storage of, processing of and access to data	Measures relate to personal data	Measures relate to other types of data
France	Yes	No	No	Yes - for public sector data	Yes - for public sector data	Yes	Yes
Germany	Yes	Yes - for accounting records and invoices	No	Yes - for telecommunications metadata	No	Yes	Yes
Greece	Yes	No	No	Yes - for telecommunications metadata	Yes - for telecommunications metadata	Yes	No
Hungary	Yes	No	No	No	No	No	No
India	Currently yes, but the impact of draft laws is unclear	Yes - “sensitive personal data” must be stored in India and not elsewhere	Yes - "critical personal data" must be stored and processed in India	Yes - for payment service provider's data	Yes - for public sector data	Yes	Yes
Ireland	Yes	No	No	No	No	No	No
Italy	Yes	Yes - for VAT-related records	No	No	No	No	Yes
Japan	Yes	No	No	Yes - for public sector data	Yes - for public sector data	Yes	Yes
South Korea	No	No	No	Yes - for public sector data and mapping data	Yes - for public sector data and mapping data	Yes	Yes
Latvia	Yes	No	No	No	No	No	No
Lithuania	Yes	No	No	No	No	No	No
Luxembourg	Yes	No	No	Yes - for the financial services sector	Yes - for the financial services sector	Yes	Yes
Malaysia	No	No	No	No	No	No	No
Malta	Yes	No	No	No	No	No	No
Mexico	No	No	No	No	No	No	No
Netherlands	Yes	No	No	Yes - for public sector data	No	Yes	Yes

Country	Data can be transferred to countries offering "comparable" protection	Economy-wide requirements for local storage of data (but not local processing of or local access to data)	Economy-wide requirements for local storage of, processing of and access to data	Sector-specific requirements for local storage of data (but not local processing of or local access to data)	Sector-specific requirements for local storage of, processing of and access to data	Measures relate to personal data	Measures relate to other types of data
New Zealand	Yes	Yes - for accounting and tax records	No	No	No	No	Yes
Poland	Yes	No	No	Yes - for gambling sector data	Yes - for gambling sector data	Yes	Yes
Portugal	Yes	No	No	No	No	No	No
Romania	Yes	No	No	Yes - for gambling sector data	No	Yes	Yes
Russia	Yes	Yes - a copy of personal data about Russian citizens must be stored in the country	No	Yes - for telecommunications data and metadata	Yes - for payment system provider's data	Yes	Yes
Singapore	Yes	No	No	Yes - for public sector data	Yes - for public sector data	Yes	Yes
Slovak Republic	Yes	No	No	No	No	No	No
Slovenia	Yes	No	No	No	No	No	No
South Africa	Yes	No	No	No	No	No	No
Spain	Yes	No	No	No	No	No	No
Sweden	Yes	Yes - for accounting records	No	Yes - for financial services sector	Yes - for public sector data	Yes	Yes
Switzerland	Yes	No	No	No	No	No	No
United Kingdom	Currently yes	Yes - for accounting records	No	Yes - for health (NHS) data	No	Yes	Yes
USA	Yes	No	No	No	No	No	No
Vietnam	Currently yes, but new data protection laws are being drafted	Yes - a copy of all data generated in Vietnam must be stored in the country	No	Yes - for online publishers, social networks and online games	No	Yes	Yes

Source: Frontier Economics analysis.

2.2 Data localisation and provisions in trade agreements

2.2.1 Background and context: World Trade Organization (WTO) provisions and data localisation

The purpose of free trade agreements (FTAs) is to provide a legally binding basis for trade partners to extend liberalisation between parties on a preferential basis over and above the treatment parties have committed to each other via their membership of the WTO. It is therefore useful to consider what requirements, if any, can be found under WTO rules that apply to data and data localisation more specifically.

2.2.2 The main body of multilateral trade rules relating to localisation is the General Agreement on Trade in Services (GATS)

The WTO agreement most relevant to data and data localisation is the GATS. The GATS imposes a general obligation to accord "most favoured nation" (MFN) treatment to all its partners on all measures affecting trade in services. It then requires WTO members to make specific commitments to eliminating limitations to market access and limitations on national treatment (i.e. the extent to which countries can discriminate between national and non-national services suppliers). The commitments apply to the sectors designated by the country and the designated modes of supply. A commitment under the GATS can be interpreted as a commitment to a minimal degree of liberalisation: a country can liberalise beyond that level either unilaterally (in which case liberalisation must be applied to all WTO members in line with the MFN obligation) or preferentially under a FTA.

There are no cross-cutting disciplines on data, but sector-specific commitments are possible

There are no explicit cross-cutting prohibitions on data localisation under the GATS. However, specific commitments in services sectors can entail a commitment to liberalising data flows. For example, computer services are one sector in which countries can make commitments, (specifically in relation to data processing and database services). The implications for data liberalisation depend on the scope of the commitments.

Suppose a country states that there are no limitations on market access and national treatment on modes 1 (cross-border supply) and 2 (consumption abroad) for data processing or database services. This means, subject to the qualifiers set out below in the discussion on exemptions, that a supplier based in country A can provide these services to residents of country B without establishing a physical presence there and, likewise, that residents of country B can access these services in country A, which would involve the transmission of data.

Most developed countries, including most EU member states, Japan, Canada and the USA have undertaken such commitments. While this entails a degree of liberalisation, the force of these commitments is considerably narrowed by the specification that these commitments apply to computer services and not to services enabled by computing (e.g. professional services, construction services or financial services).

Two areas in which WTO rules per se (as opposed to specific commitments) contain provisions relating to cross-border data flows are:

- The Understanding on Financial Services. Article 8 stipulates a positive obligation to eliminate restrictions, as of the date of entry into force of the agreement, on transfer of information and processing of financial information … *necessary for the ordinary businesses of a financial services supplier* (emphasis added). This is counterbalanced in the same article by exemptions for privacy, confidentiality and personal data protection (subject to the requirement that these reasons are not invoked to circumvent commitments).[4]
- Annex on Telecommunications (Article 5) requires members to allow suppliers from other members to use networks for the transmission of information including that stored in databases.

Any commitments to data liberalisation can be counterbalanced, at least in part, by general exemptions for policy purposes

In addition to the provisions under the specific provisions described above, the GATS also allows governments to deviate from their obligations for specific public policy purposes. GATS Article XIV(c)(ii) specifies the privacy of individuals in relation to the processing and dissemination of personal data as one of these exemptions. These exemptions are subject to a necessity test, i.e. that they are not more trade restrictive than necessary to achieve the policy objectives, and that they cannot entail "unjustified discrimination" or a "disguised restriction on trade".

In sum, the GATS contains relatively limited disciplines on data localisations. Those that are present are sector specific; may be limited by the scope of the commitments undertaken; and are subject to balancing provisions that allow for policy action to secure wider public policy objectives. These balancing provisions nevertheless do incorporate disciplines on the way in which governments can deviate from their obligations by subjecting policy measures to a necessity test and requiring that they are not a disguised form of discrimination or protectionism.

In general, current WTO rules are relatively weak constraints on the ability of member countries to introduce data localisation measures should they choose to

One of the upshots is that current WTO rules generally do not limit the extent of the discretion governments have to introduce data localisation requirements should they chose to. A key question in turn is whether commitments under FTAs are able to go beyond the WTO baseline – in particular, whether FTAs introduce commitments that reduce the extent to which a government is able to introduce data localisation measures, at least insofar as these restrictions affect trade between signatories to the FTA.

2.2.3 Examples of FTAs and their treatment of data localisation

As observed above, a central question is how much further than WTO rules do FTAs go in imposing disciplines on data localisation, i.e. to what extent do they contain rules that mandate the elimination of such requirements, on what basis, and how are any counterbalancing provisions (i.e. to secure policy objectives) framed. Table 1 below provides an explanation of

[4] Whether a measure is pursued for public policy reasons or for circumvention is a matter of interpretation. In the event of a dispute, it is likely that rulings would err on the side of giving the country in question latitude to define its policy objectives, particularly in the context of financial services where prudential regulatory measures are the subject of a carve-out.

the data-related provisions in some of the main FTAs (or bespoke data arrangements) involving the countries of interest to this study.

Table 1 Overview of selected FTAs and bilateral data provisions

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
Australia-Japan	No explicit prohibition of restrictions on data flows in e-commerce chapter. Restates Article 8 of the GATS. Understanding on financial services and provisions of annex on telecommunications.	E-commerce chapter. Commitments to protecting personal data in line with international standards. General exemptions along the lines of GATS Article XIV(c).	No additional liberalisation relative to GATS. Reference to international standards may provide some discipline for discretionary imposition of localisation for data protection purposes.
Australia-South Korea	Similar to AU-Japan	Similar to AU-Japan	Similar to AU-Japan
Australia-Singapore Digital Economy Agreement	Similar to CPTPP commitments (see below). Includes additional disciplines prohibiting computing localisation requirements for financial services.	Allowance for measures to pursue legitimate interests (note: no explicit necessity test), but requirement that measures do not constitute unjustifiable discrimination or a disguised restriction on trade Recognition that parties have own regulations governing data protection. Commitment to developing a framework for the protection of personal information' General exemptions along the lines of GATS Article XIV(c)'.	Additional liberalisation relative to baseline through inclusion of specific prohibitions on localisation. Counterbalancing provisions include GATS language on avoiding unjustifiable discrimination and disguised restriction on trade, but no inclusion of necessity test suggesting relatively significant residual scope for discretion . Possibly moderated by development of a framework for personal information protection.
CPTPP (Comprehensive and Progressive Trans-Pacific Partnership)	Article 14.11.2 specifies a positive obligation to allow cross-border data flows, including personal data, for the purposes of conduct of business of a "covered person".[5] Article 14.13 prohibits	Counterbalanced by exemptions in 14.1.1(3) which allow measures to pursue legitimate public policy objectives provided: (i) not being a means of arbitrary or unjustified	Additional liberalisation relative to baseline through inclusion of specific prohibitions on localisation. Counterbalancing provisions include GATS language on avoiding unjustifiable discrimination and disguised

[5] A covered person means an investment, investor or service suppliers other than financial services suppliers or financial institutions.

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
	requirements on use or location of computing facilities in a party's territory as a condition of business. For financial services providers, provisions require parties to transfer data for processing if this is required in ordinary course of business.	discrimination and a disguised restriction on trade, and (ii) not being more restrictive on transfer than is required to achieve the objective. Recognition that parties have their regulatory requirements concerning information transfer. For financial services, allowance of measures to protect personal data, privacy and confidentiality; also requires authorisation from regulator for transfer to a designated enterprise. Anti-circumvention following GATS. General exemptions along the lines of GATS Article XIV(c).	restriction on trade. Use of "required" rather than "necessary", when the latter is an established expression in trade agreements, raises some questions as to whether this wording weakens disciplines on use of counterbalancing measures. Exemptions for financial services quite broad and no necessity test.
EU-Japan	A "rendez-vous" clause committing parties to reassess need for provisions on free flow of data three years after entry into force of the agreement.	Recognition of importance of maintaining protection of personal data in accordance with the laws of the parties. General exemptions along the lines of GATS Article XIV(c).	No additional liberalisation and wide latitude for conditional localisation for the purposes of personal data protection. In the event, EU considered Japan's data personal data protection to be GDPR adequate, and Japan recognised EU regime as equivalent.
EU-Canada (CETA)	Chapter on e-commerce does not mandate free flow of data. Restates Article 8 of the GATS. Understanding on financial services and provisions of annex on telecommunications.	Provisions on e-commerce stipulate " best endeavours" to protect personal data, requiring that such endeavours take account of international standards.	Reference to international standards for personal data protection potentially reduce scope to some extent for discretionary policy action.

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
		General exemptions along the lines of GATS Article XIV(c).	
EU-South Korea, EU-Singapore	Cross-border services trade commitments include liberalisation commitments on data processing, data storage, data hosting or database services. Restates Article 8 of the GATS. Understanding on financial services and provisions of annex on telecommunications.	E-commerce chapter includes provisions that e-commerce development must be fully compatible with international standards on data protection. General exemptions along the lines of GATS Article XIV(c).	Reference to international standards for personal data protection potentially reduces scope to some extent for discretionary policy action.
EU-Mercosur	Computer service lists data processing and data storage as services which are subject to commitments on elimination. Limitations on market access and national treatment. Whether this liberalises cross-border data flows depends on nature of actual commitments undertaken (yet to specified).		Limited
EU-UK Trade and Cooperation Agreement (TCA)	The TCA contains a chapter on Digital Trade. Article 201, commits both parties to ensuring cross-border data flows to facilitate trade, and proscribes measures to restrict data flows. Proscribed measures include: ▪ Requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network	Article 202 states that "each Party recognises that individuals have a right to the protection of personal data and privacy…". It also says that nothing in the agreement shall prevent parties from "adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under	Broad-ranging commitments to data liberalisation with an explicit recognition of their trade-facilitating effects. The balancing of Article 201 by Article 202 reflects EU horizontal provisions (see below), though its scope is narrower. At present, bilateral cross-border personal data flows between the UK and the EU are secured by reciprocal adequacy determinations. In the absence of adequacy, other personal data transfer mechanisms that apply on a case by case basis are

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
	elements that are certified or approved in the territory of a Party; ▪ Requiring the localisation of data in the Party's territory for storage or processing; ▪ Prohibiting the storage or processing in the territory of the other Party; or ▪ Making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.	conditions of general application for the protection of the data transferred". In practice, the provisions of the article allow for decisions or measures that could facilitate cross-border data flow, including adequacy or other mechanisms, such as standard contractual clauses, that are provided for in the GDPR.	available, but may impose higher compliance costs than if adequacy were achieved.
EU – horizontal provisions for future FTAs	Part A sets out prohibitions: on requiring use of computing and network facilities in a territory as a condition of processing; on localisation of data for storage or processing; on prohibiting storage and processing in territory of another party; on making cross-border transfers conditional on localisation requirements or use of computing facilities.	Part B sets out counterbalancing provisions by stipulating that data privacy is a *fundamental right* and presenting the safeguarding as a general exception, i.e. parties can maintain safeguards they deem appropriate.	Part A goes beyond requirements on data localisation in current EU FTAs and, if agreed with partners, would support much deeper liberalisation commitments than under GATS or current practices. But Part B heavily qualifies the effects of Part A: it makes liberalisation conditional; on parties adopting an approach to personal data protection similar to EU's (based on fundamental right principles). This reflects ECJ rulings on US privacy shield. In principle this may make it more difficult to strike liberalising provisions in FTAs with the EU; and could potentially also allow the ECJ

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
			to reverse liberalising provisions if deemed not to safeguard fundamental rights
RCEP (Regional and Comprehensive Economic Partnership)	Two articles: 12.14 dealing with the location of computing facilities and 12.15 dealing with cross-border transfer of information by electronic means. Both recognise regulatory requirements including safeguarding security and confidentiality (computing storage). 12.14(2) prohibits making location of computing facilities in a territory a condition of conducting business. 12.15(2) prohibits preventing cross-border transmissions needed for the conduct of business. (Time-limited exemptions for Cambodia, Myanmar, Laos and Vietnam). Preamble to section specifies that this section deals with electronic commerce and specified limitations in its applicability to cross-border services trade and investment.	12.14(3) and 12.15(3) are counterbalancing requirements allowing restrictions a party considers necessary for legitimate public policy objectives as long as not arbitrary or unjustifiable discrimination or a disguised restriction on trade. They add a further provision regarding the protection of essential security interests. A footnote explains that necessity of the legitimate objective is decided by the implementing party. General exemptions along the lines of GATS Article XIV(c).	Liberalisation beyond GATS baseline through the prohibitions. But the broad nature of the balancing provisions, especially the discretion allowed to parties to determine what is necessary to pursue a legitimate public policy interest, may limit the extent of this incremental liberalisation and impact current policy and practices.
NZ-Chile-Singapore Digital Economy Partnership	Restates CPTPP provisions on data (Article 4.3)). CPTPP provision on prohibition of localisation requirements for computing also included.	CPTPP balancing requirements, but also adds a specific set of commitments on developing a framework for the protection of personal information (Article 4.2) General exemptions along the lines of GATS Article XIV(c).	Additional liberalisation relative to baseline through inclusion of specific prohibitions on localisation. Counterbalancing provisions include GATS language on avoiding unjustifiable discrimination and disguised restriction on trade, but no inclusion of necessity test suggesting relatively significant residual scope for discretion . Possibly moderated by development of a

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
			framework for personal information protection.
UK-Japan	Financial services: prohibition of stipulations requiring localisation of computing facilities. Prohibition on restrictions of cross-border data transfers for the conduct of business by a covered person. Prohibition on requiring localisation of computing facilities as a condition of conducting business.	Financial services: can use localisation requirements if otherwise unable to access information "appropriate" for regulatory functions subject to consultation with regulatory counterparts and opportunity to remedy lack of information. General cross-border data flows: can deviate from general prohibition on restrictions to achieve legitimate public policy objective provided it is not unjustifiable/arbitrary discrimination or disguised restriction on trade; and restrictions on transfer not "greater than required" to meet objective. Prohibition on computing localisation includes permission to deviate to take measures "necessary" for legitimate public policy, provided not arbitrary or unjustified discrimination or disguised restriction on trade.	Language goes beyond what is in the EU-Japan treaty which UK was part of prior to leaving EU. Language on financial services similar to Australia-Singapore agreement, while balancing provisions also include elements resembling USMCA. Language on data similar to CPTPP. On balancing: use of "appropriate" in allowing localisation requirements for financial services suggests lower hurdle to clear than if necessity used. Balancing for general data flows also follows CPTPP approach and does not explicitly use "necessity". Balancing for localisation of computing facilities uses standard necessity test.
United States-Mexico-Canada (USMCA) Agreement	Positive obligations to eliminate barriers to data flows: Article 19.11(1) requires an elimination of barriers to cross-border	Specific counterbalancing measures apply to Article 19.11(1) and allowance to take "necessary" for	Significant strengthening of liberalisation vis a vis GATS baseline and current practices (notably in Mexico) through wording of

Agreement	Provisions addressing data localisation/ mandating freedom of cross-border data flows	Counterbalancing provisions relating to data protection	Effects relative to GATS/ WTO baseline and implications for current policy settings
	data flows. Article 19.11(2) prohibits use or location of computing facilities in the territory as a condition of business in that territory. Specific provisions for financial services prohibiting restrictions on data for the conduct of business of a financial services provider, and prohibition of requirements to localise computing facilities.	legitimate public policy requirement. Prohibition of localisation of computing facilities not explicitly counterbalanced. Reference to Asia-Pacific Economic Cooperation (APEC) cross-border privacy rules as way of balancing cross-border flows with information requirements. Balancing provisions for financial services broadly formulated to allow protection of personal data and privacy. Regarding localisation of computer facilities: requirement of access to information for financial supervisory reasons. General exceptions under Article 32.1 of the agreement provide for the application of GATS Article XIV.	prohibitions. Inclusion of necessity tests in counterbalancing provisions reduce scope for discretionary localisation requirements.
US-South Korea	Best endeavours commitment to refrain from imposing or maintaining unnecessary barriers to the flow of electronic information.	General exemptions along the lines of GATS Article XIV(c).	Modest increase relative to GATS baseline; scope for discretion still maintained.
US-Singapore	**As above**	**As above**	**As above**

2.3 Implications of trade provisions for an analysis of data localisation

The analysis suggests there are two principal issues that determine the impact of trade provisions cross-border data flows, and, specifically, how far these are constrained by measures taken by countries:

- The scope and stringency of prohibitions in these agreements that apply to restrictions on cross-border data flows and/or on requiring the localisation of computing facilities as a condition of doing business; and
- The manner of formulation of balancing requirements that allow countries to pursue public policy interests, notably data protection, and specifically how these interact with the provisions mandating cross-border data flows and/or prohibiting restrictions (e.g. whether these are seen as exemptions subject to specific conditions or provisions that are intended to override data liberalisation provisions).

These sets of issues can be in tension with each other. How this tension plays out depends on the framing of commitments on eliminating restrictions on cross-border data flows, and on the extent to which governments undertaking measures to pursue legitimate public policy objectives are required to demonstrate that these are not more trade restrictive than necessary and are not an arbitrary form of discrimination or a disguised restriction on international trade.

There is considerable variation in how far different agreements address both sets of issues. At one end EU-Japan, EU-South Korea and US-South Korea offer relatively weak incremental commitments (relative to GATS baselines) on the prohibition of localisation requirements and restate (in the case of the two EU FTAs cited) a general commitment to protection of personal data.

The CPTPP provisions (on which other arrangements, notably the UK-Japan FTA, and the bespoke digital agreements involving Chile, New Zealand, and Singapore, and Australia and Singapore, build upon) go significantly beyond GATS commitments in terms of the phrasing of the prohibitions on localisation requirements. The counterbalancing test does not include an explicit reference to the “necessity” of any measure taken to protect personal data; and stating instead that measures must not be more restrictive than is required. The concept of necessity in international trade jurisprudence is not fully settled, but it does at the very least require the country implementing the measure to demonstrate that the measure contributes to the policy objective sought and is not more trade restricting than alternatives that could have the same effect. This in turn provides a discipline on measures taken and is supportive of liberalisation.

The bilateral agreements that reflect or build on the CPTPP, (including the UK’s FTA with Japan and the bespoke digital agreements described above) go further on data transfers for financial services. This includes specific prohibitions on restrictions for cross-border data flows and on the requirement to locate computing facilities in the territory of the country being supplied.

The tension between data liberalisation requirements and counterbalancing provisions is probably strongest in the RCEP agreement. The RCEP essentially reproduces CPTPP commitments on liberalisation. But it not only allows for measures necessary to secure a public policy objective, it leaves the definition of necessity entirely to the discretion of the

implementing party. Taken at face value, it is difficult to judge whether this will allow, in practice, for a greater level of liberalisation relative to the GATS or to current practice.

On balance, the provisions in the USMCA seem to have the most force in securing liberalisation over and above the existing GATS baseline and in terms of actual practices on the ground. This is because of both the scope and stringency of provisions prohibiting localisation and the tighter formulation of the counterbalancing provisions through the inclusion of an explicit necessity test. Even for relatively liberal data regimes such as the USA's, the implementation of these provisions would curtail the scope for discretionary increases in the levels of data localisation restrictiveness.

The EU horizontal provisions,[6] which the EU may seek to implement in future FTAs, also bring a new dimension to the tension between liberalisation commitments and counterbalancing provisions. Part A of the horizontal provisions goes beyond the commitments in existing EU FTAs that require the elimination of restrictions on cross-border data flows. At the same time, Part B defines data protection as a fundamental right and authorises parties to take any appropriate action to safeguard this right.

The practical policy impact of data provisions also needs to take account of the fact that (as in most services trade matters) actual country practices are more liberal, often significantly, than the GATS/WTO commitments. The value of a FTA is that it can provide legal security to partners by acting as a standstill/lock-in mechanism, i.e. the provisions limit how far a country can scale back actual liberalisation and/ or impose future restrictions, as far as its FTA partners are concerned.

Finally, as with the GATS, the transfer of data and information for financial services is treated differently to data in general. Indeed, the FTA texts discussed above usually explicitly state that financial services are not covered by the general provisions regarding data. The approach taken across most major agreements, notably CPTPP and USMCA, is to require cross-border data flows necessary for the conduct of business. The CPTPP, and agreements that build on them, as well as the USMCA go further than the GATS by also including prohibitions of regulations that would require financial services providers to use computing facilities located in the territory they serve as a requirement for doing business.

Balancing provisions for financial services are relatively broadly framed, in keeping with the wider scope of discretion afforded to financial services regulation and regulators for prudential purposes. The UK-Japan agreement potentially goes further than others in incorporating a necessity test for measures that might impose localisation of computing facilities.

[6] https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

3 COUNTRY DEEP DIVES

3.1 Introduction

The previous sections presented an overview of data localisation requirements internationally. They also reviewed the impact of trade agreements on data governance and localisation practices. We concluded that trade agreements can limit the scope of countries to arbitrarily impose restrictions (i.e. as a disguised restriction on international trade and outside defined public policy objectives), though the extent to which such agreements can act as restraints varies depending on the drafting of the provisions.

In this section, we consider in more detail the extent and approach taken to data restrictions in specific countries and present an evaluation of the effects of these policies. The countries selected are: China, France, India, Japan, South Korea, Mexico and the USA. We also provide an analysis for the EU. The selection reflects prevailing trade patterns (with the EU and the USA being the UK's largest trade partners), and different levels of development.

The sections provide an analysis of the nature and rationale for data localisation requirements in these jurisdictions. They then proceed to evaluate the impacts of data localisation (and, conversely, of liberalising cross-border data flows). In order to do this, we represent data localisation as an increase in policy restrictiveness on cross-border data flows. We then model the effects of the increase of this restrictiveness on the cross-border trade of goods and services.

The intuition is that data flows facilitate trade. This is particularly the case with the emergence of cross-border value chains as a key driver of international trade in which different stages of the production process are coordinated across different countries and which involve a high degree of integration between services and manufacturing activities. In such a context, restrictions on cross-border trade add to trade costs, in a manner analogous to tariffs and non-tariff measures.

Details of the modelling approach are provided in Annex A. The key steps are as follows:

- We represent changes to data localisation as changes to the Organisation for Economic Co-operation and Development's (OECD) Services Trade Restrictiveness Index (STRI) and, specifically, the elements in this index that relate to data localisation.
- We use a gravity model of trade which includes the STRI as one variable explaining bilateral trade flows in order to capture the effects of changes in data restrictiveness on trade in the countries of interest.
- We model the effects on sectors and activities that are deemed to be data intensive. These are:
  - Services sectors, including IT and telecoms, which contain data-enabled businesses; publishing, financial services, transportation and storage; and wholesale, retail and business services (such as accounting and legal services).

- High value-added manufacturing, which includes activities such as automotives, electrical machinery and computing (see Annex A for further details) . These are sectors that typically display a high degree of integration between services and goods.

Modelling involves measuring the impact of a policy change relative to a baseline. In this case, our focus is on analysing the impacts of data localisation policies. As observed in section 2.1 and in the following sections, one challenge is that policies related to data localisation and data governance are not static, and indeed are currently subject to review and revision. This is true at both the national level and in relation to international cooperation.

We therefore adopt the following approach:

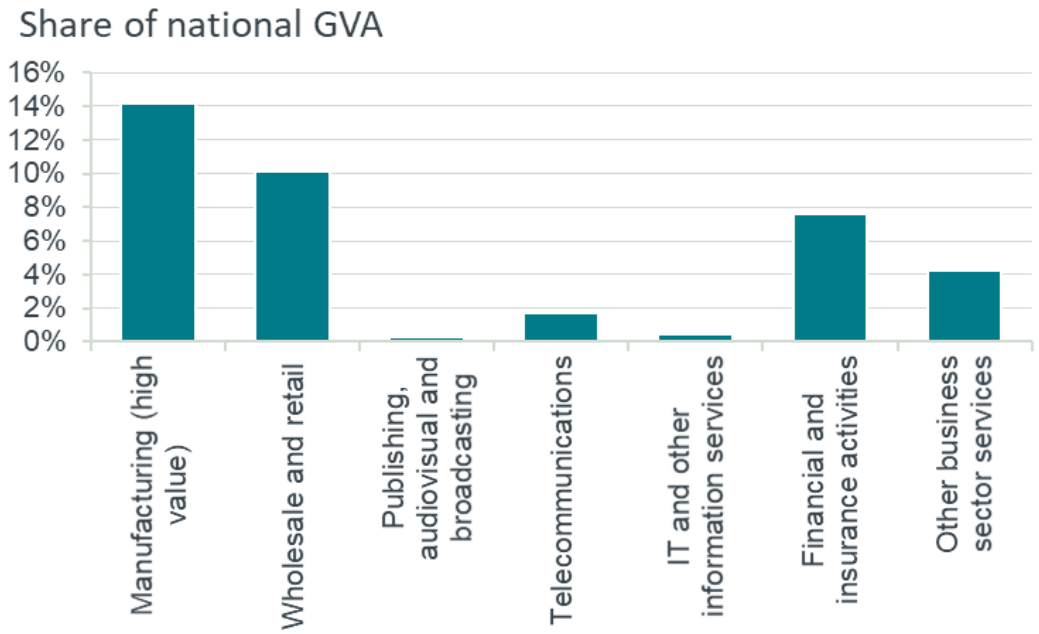
- First, we model the effects of having the country of interest and its partners move from current policy settings to a high level of restrictiveness on cross-border data flows. Under this scenario, the local storage of data is mandated and the cross-border transfer of data for storage overseas is prohibited. This captures several insights from the analysis in the preceding sections:
  - Approaches to cross-border data flows have been relatively liberal, but there are increasing pressures in favour of localisation, whether absolute or conditional.
  - Outside of specific FTAs, current rules give a large measure of discretion to countries to pursue data localisation, including the types of conditions they set on cross-border data flows.
  - This scenario captures the value at risk to the countries of interest from their own attempts at data location and those by partners.
- Second, beginning with the fully restricted settings described in the first scenario above, we model a hypothetical scenario in which the countries of interest and the EU enter into reciprocal bilateral agreements that secure free cross-border flows of data.
  - The difference between scenario 1 and scenario 2 reflects the value of these bilateral reciprocal arrangements in securing free cross-border flows of data.
  - The residual impacts on trade after the adequacy reflect the effects of restrictions in place on data flows vis a vis non-EU countries, as these are not assumed to change relative to scenario 1.

3.2 China

3.2.1 Country background

Figure 6 shows the contribution of each data-intensive sector to China's GVA. The data-intensive sectors collectively account for 39% of China's GVA, with the most significant sectors being high-value manufacturing (14% of GVA), wholesale and retail (10%), and financial and insurance activities (8%).

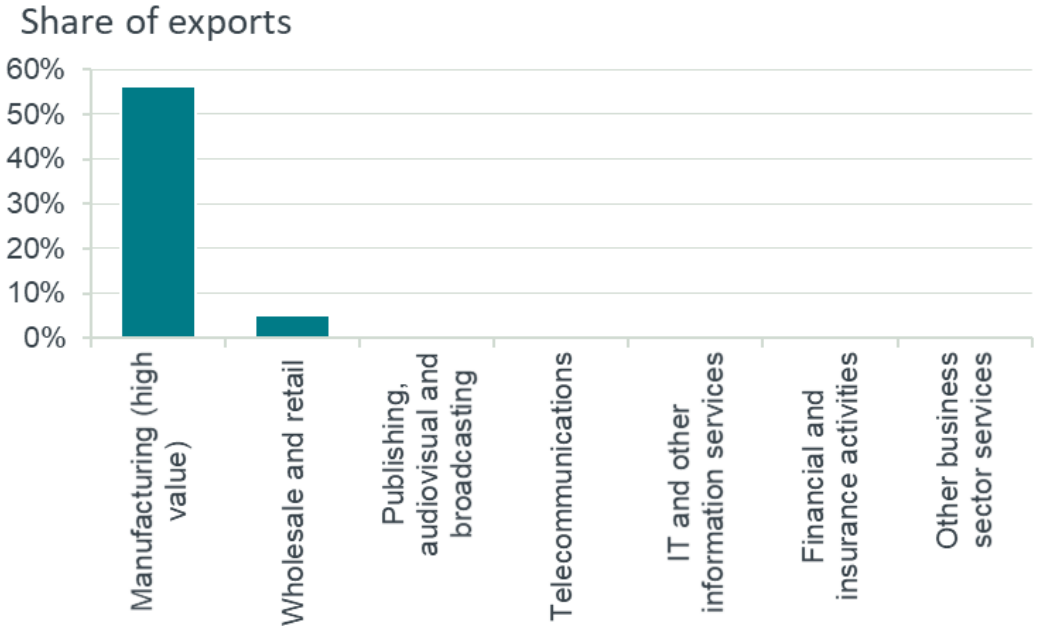
Figure 6 Share of China's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 7 shows each data-intensive sector's share of China's exports. The data-intensive sectors collectively account for 62% of China's exports by value. The most significant data-intensive sector is clearly the high-value manufacturing sector; it accounts for 56% of the value of China's exports. The wholesale and retail sector accounts for 6% of China's exports, and the remaining data-intensive sectors do not make a significant contribution to China's exports.

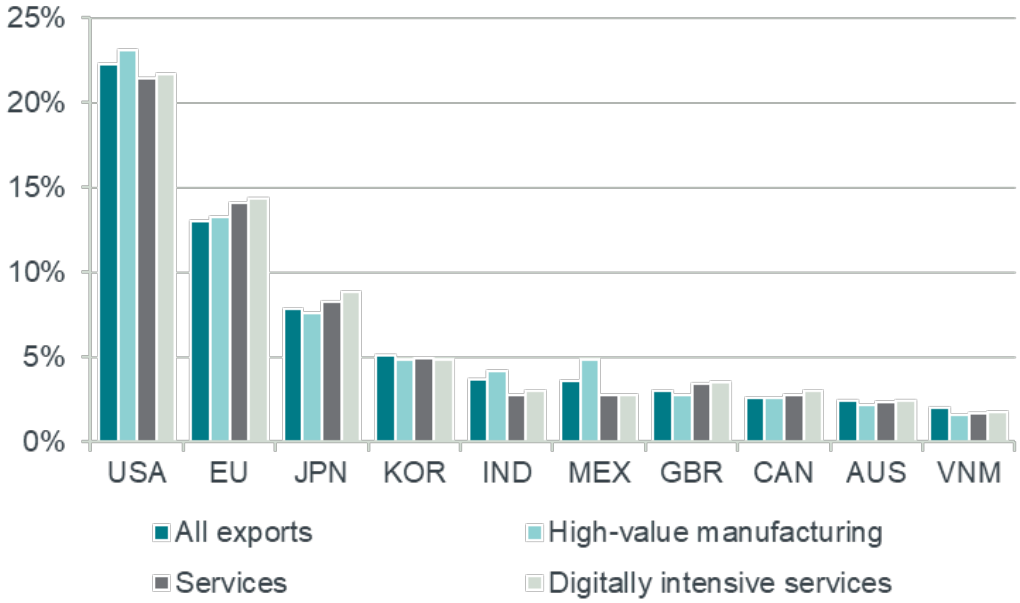
Figure 7 Share of China's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 8 shows China's ten largest trading partners (based on the value of exports received by partners). The USA is by some distance China's largest export market. The UK is China's seventh largest trading partner based on all exports, but it is China's fifth largest trading partner based on both services and digitally intensive services. The UK is the recipient of 3% of Chinese exports and 4% of Chinese exports for digitally intensive services.

Figure 8 China's ten largest trading partners (percentage share by partner for export category)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.2.2 Domestic legal and policy framework

The Chinese legal framework governing cross-border data transfers and data localisation is a patchwork of various laws, regulations and national standards. Despite the complexity of the legal framework, the implication is straightforward: data localisation is the default and cross-border transfers are the exception. China thus has a very restrictive policy stance on cross-border data flows, and this is not limited to personal data.

The Cybersecurity Law, passed in November 2016, is China's first "comprehensive and fundamental" law concerning the internet.[7] It is also the law which instituted the country's current cross-border data flow regime (which is based on prior established practice). Before any "personal or important information" (defined below) can leave China, the transferor must first complete a security assessment and seek approval from the relevant authority. Certain data controllers (critical information infrastructure (CII) operators) must store a copy of their "personal and important information" in China.

[7] Jinhe Liu (2020), "China's data localization", Chinese Journal of Communication, 13(1): 84-103.

More specifically, the law covers personal information (defined as data identifying or reflecting the activities of a certain natural person) and important information (defined as data concerning national security, economic development and societal and public interests). The law covers all network operators but has specific provisions for CII operators. The scope of CII operators is defined by supporting regulation, not the Cybersecurity Law itself, and includes sectors such as finance, energy, media, telecommunications, public services, defence and technology. All network operators must have an approved security assessment in place before transferring data abroad. The security assessment concerns matters of national security, public interest and personal information security. CII operators can also transfer data abroad (subject to assessment), but they are also required to store a local copy of personal and important information.

In addition to the general data transfer framework, China has stipulated a number of data localisation measures which apply to specific sectors and types of data. This started in 2011 when the People's Bank of China issued a notice prohibiting the overseas processing, storage or analysis of the personal financial data of Chinese citizens. Similar measures have also been introduced covering the insurance sector. In addition, health data must be stored and processed in China, and the transfer of such data overseas is prohibited. Sector-specific regulations also cover non-personal data: data related to online navigation services and map databases are required to be stored in China, and taxi and ride-sharing services must store all their data in China with Chinese services providers.

Balancing trade benefits with other public policy objectives

It is clear that the primary focus of China's data governance framework is on public policy matters, specifically national security. China's data flow regime is motivated principally by the desire to maintain cyber security and thus national security; "security is the most important and direct issue".[8] Other questions, including the possible benefits of data transfers on trade, are subordinate to these concerns and the authorities wish to retain as much discretion as possible in regulating data flows to achieve their overarching objectives.

In addition to national security concerns, China regards data as "an important basic strategic resource for the country", and thus worth protecting in its own right.[9] Self-sufficiency in science and technology is an important objective of the 13th Five-Year Plan for National Informatization. Data localisation can support this objective by helping to foster China's domestic data industry.

China's restrictive approach to cross-border data flows is also consistent with its wider internet policies. The control China exerts over local access to the internet is thought to be more sophisticated than in any other country. China is more easily able to exert this control if the data underlying digital services available in the Chinese market are stored within the country's borders.

[8] *Ibid.*

[9] Outline of the 13th Five-Year Plan for National Economic and Social Development of the People's Republic of China, NPC & Central Committee of the CPC, March 2016; The Action Outline for Promoting the Development of Big Data, the State Council of PRC, August 2015.

3.2.3 Free trade agreements

China is a signatory to the RCEP (Regional and Comprehensive Economic Partnership) agreement which contains provisions concerning data localisation and cross-border data flows. However, the structure of the commitments suggests that the agreement does not contain strong disciplines that would limit the scope China has to restrict data flows on a discretionary basis.

Article 12.14(2) prohibits requiring the use of local computing facilities as a condition of doing business in a country, while Article 12.15(2) prohibits preventing cross-border data transfers needed for the conduct of business. These two provisions are subject to counterbalancing requirements which allow data localisation requirements and cross-border data transfer restrictions that are necessary for legitimate public policy objectives, provided that the measures are not arbitrary or unjustifiable discrimination or a disguised restriction on trade.

While this language contains similarities to provisions used in other trade agreements, such as the CPTPP and WTO provisions, it diverges in important respects. Crucially, it would be for each individual signatory to determine what measures are necessary for their legitimate policy interests. This makes it difficult, if not impossible, for a party to RCEP to challenge measures taken by another party on the grounds that these measures are not necessary. This in turn means that China, and all other RCEP signatories, would have ample scope to continue to introduce and maintain data localisation measures and cross-border data restrictions regardless of Articles 12.14(2) and 12.14(2) of RCEP. It is likely that this flexibility was the price needed to get China to sign up to the commitments in the first place.

3.2.4 Modelling the impacts of data localisation

In this section, we estimate how changes to restrictions on cross-border data flows affect the value of China's trade under two scenarios.

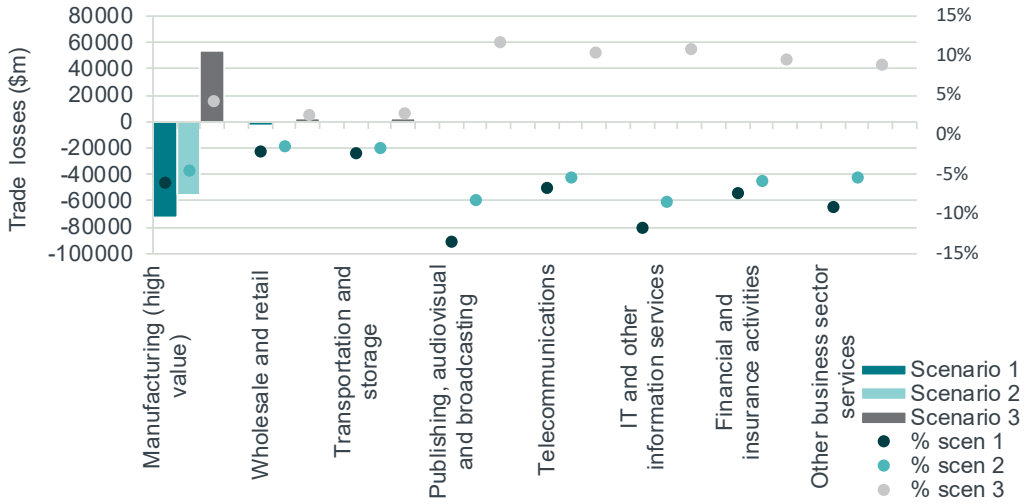
In the first scenario, we assume that China and its trading partners move from their current practices to full data localisation. This provides an estimate of the value at risk for the economies. This move to full localisation would be (largely) consistent with GATS, and so this analysis can also be interpreted as the value of "locking in" current levels of liberalisation (for example, through a FTA), though, admittedly, given China's high existing levels of restrictiveness, this locking-in effect would not be substantial.

In the second scenario, we assume that China then moves from the full data localisation situation under scenario 1 agreeing reciprocal data arrangements with the EU.

Finally, given that China is a highly restrictive country in terms of cross-border data flows, we model a third scenario in which it liberalises its own data restriction, i.e. it moves from its current level of restrictiveness to a level of restrictiveness equal to the median restrictiveness of countries for which STRI scores are reported. It could do this either unilaterally or in the context of trade agreements (e.g. RCEP).

Figure 9 below shows the trade losses for data-intensive sectors from these scenarios. The bars represent the absolute loss of trade (in $m, as measured by the left-hand vertical axis), and the dots represent the percentage loss of trade (as measured by the right-hand vertical axis).

Figure 9 Trade impact of data localisation modelling results for China



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

As China already has a relatively restrictive approach to cross-border data flows, much of the impact of scenarios 1 and 3 on China's trade comes via changes to the restrictiveness of trade partners.

In absolute terms, the impacts of data localisation fall most heavily on high value-added manufacturing (the absolute values for other sectors are so small in comparison that they do not appear in the columns in the graph). This reflects the dominance of the sector in the composition of China's trade. Moreover, the organisation of production in these sectors in China leaves it particularly open to the effects of data localisation. Operations typically rely heavily on imported goods and services which are used as inputs into production and which are then exported either as finished products or for further processing and marketing. Such value chains are typically data intensive.

Wholesale and retail, transportation and storage account for the bulk of China's services exports. Although these sectors experience a small decrease in trade in percentage terms, the impact in absolute terms ranges from $2 billion in scenario 2 to $4 billion in scenario 1. Proportional to these trade losses, the absolute trade losses experienced by other services sectors are very small. However, the effects proportionate to the value of their own trade are substantial, particularly for publishing, audio-visual and IT.

Under scenario 2, we can see that entering into bilateral reciprocal arrangements with the EU reduces some of the losses experienced in scenario 1. But the bulk of the losses remain. This in turn suggests that from a Chinese perspective, securing commitments with non-EU trade partners to avoid rolling back from existing levels of data flow liberalisation is a priority.

Scenario 3 shows that China could gain significantly from reducing its own restrictions on cross-border data flows. High value-added manufacturing posts the

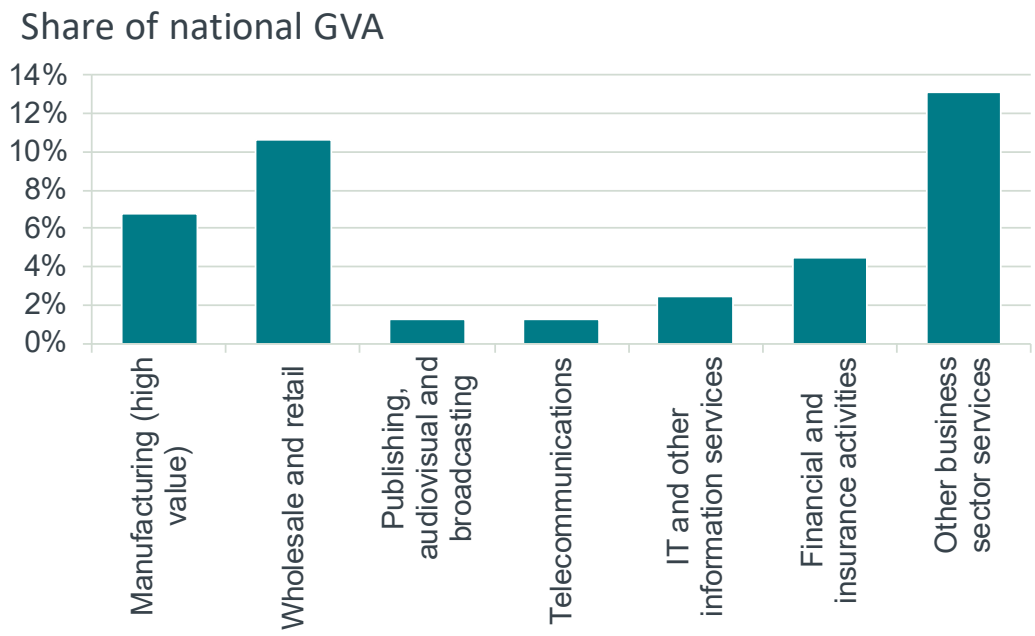
highest absolute gains. Overall, the value of the gains from unilateral liberalisation are close – in absolute value terms – to the losses generated by partners reverting to restrictive data settings. As already observed, the major trade agreement to which China is a party (RCEP) contains some disciplines on eliminating data localisation, but these are weakened by the large degree of discretion left to parties to define the conditions for restricting data flows. The results suggest that China would stand to benefit if it used its participation in arrangements such as RCEP to actively reduce restrictions on data flows.

3.3 France

3.3.1 Country background

Figure 10 shows the contributions of digital/ data-intensive sectors to French GVA. Collectively, they account for just under 40% of GVA. Other business services, which notably include professional services, legal services and accounting, constitute the single largest sector in terms of GVA.

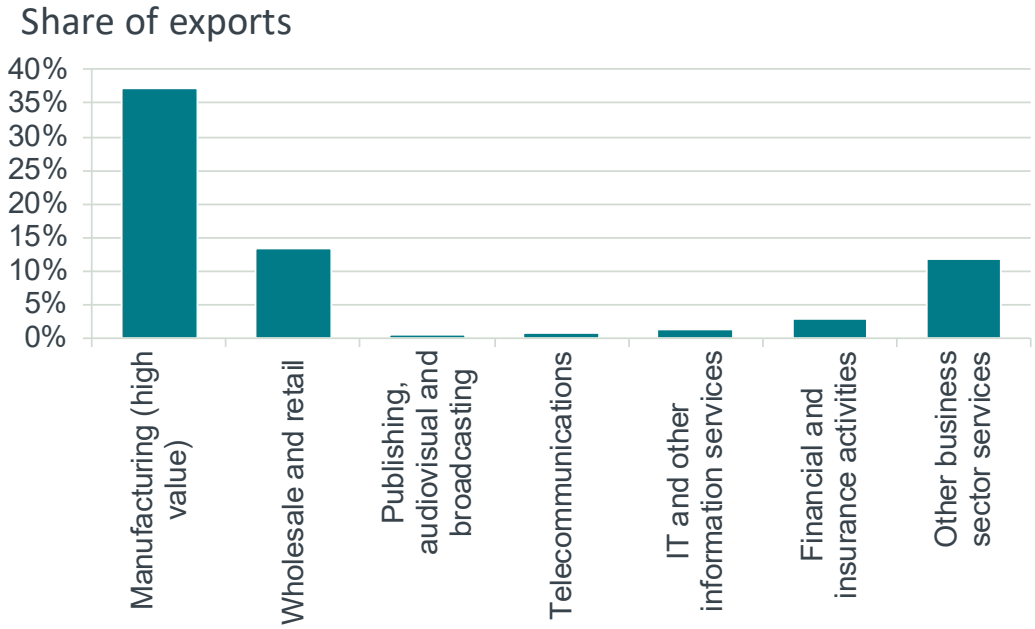
Figure 10 Share of France's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 11 reports the share of the different data-intensive sectors in French exports. The figures can be usefully compared to the GVA figures. The comparison suggests that business services and wholesale/retail services have a strong domestic focus, whereas high value-added manufacturing has a stronger export orientation given its share of GVA.

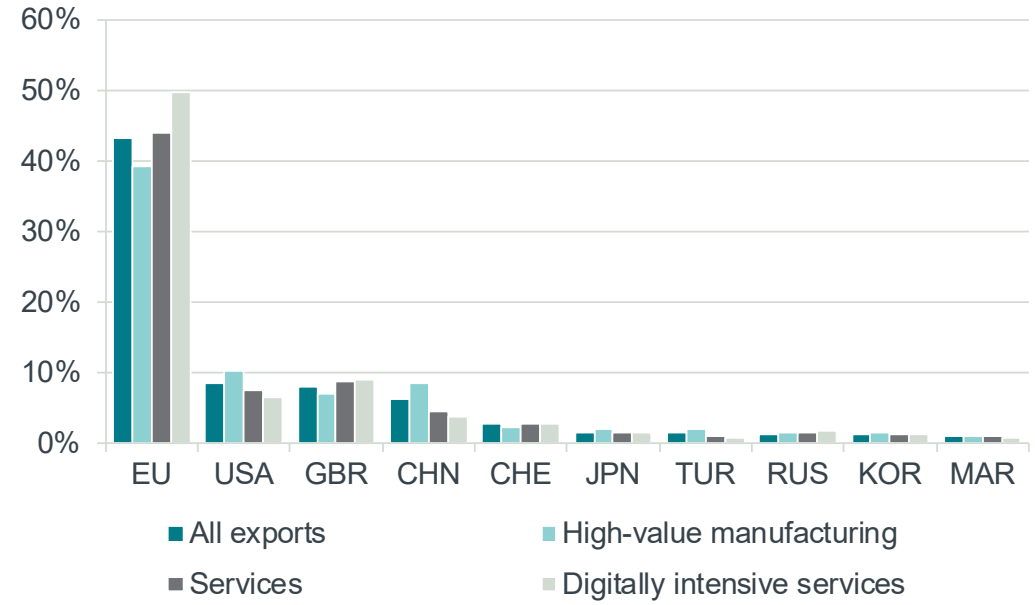
Figure 11 Share of France's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 12 presents information on France's largest trade partners. It shows that the EU is particularly important for digitally intensive services, underscoring the importance of free data flows within the EU. The UK is the other major trading partner whose share of French digitally intensive services is (slightly) higher than for other sectors.

Figure 12 France's largest trade partners (percentage share of exports by country by major category of exports)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.3.2 Data governance frameworks and localisation

Domestic legal and policy framework

The GDPR, which came into force in 2018, provides the overall framework for personal data governance in France. As an EU regulation, the GDPR is legally binding on all members under Article 288 of the TFEU. It supersedes any domestic law in case of conflict. (Please refer to the analysis in section 3.9 on the EU Deep Dive for further details).

The main French law that sets the framework for data governance is the 2018 law on personal data protection. This law updates previous data protection law (dating from 1978) to incorporate the GDPR in a French context. A decree in 2019 implementing the law further specified procedural provisions relating to the French data protection authority, as well as data subjects' rights.

The main body tasked with data protection in France is the CNIL (*La Commission Nationale de l'Informatique et des Libertés*). Under the 2019 decree, and in keeping with the ECJ's findings under the SCHREMS I case, the CNIL has the power to temporarily suspend an international data transfer outside the EU. In that case it refers the matter to the *Conseil d'Etat*, France's highest administrative court. This court is then required to refer the matter to the ECJ, which will then formulate a view on findings of adequacy or any other decision taken by the European Commission to authorise the transfer of personal data outside the EU.

The CNIL has imposed fines for the breach of GDPR provisions, notably a €50 million fine on Google in 2019. In November 2020, the Carrefour Group (supermarkets and financial services) was fined €2.25 million because, inter alia, information to customers on personal data transfers outside the EU was unclear. In December 2020, Google Ireland and Google LLC were fined €40 million and €60 million respectively because the use of cookies by google.fr was deemed to have breached the provisions of the 2018 law requiring informed consent. While not explicitly a data localisation issue, it has implications for personal data transfers. A fine of €35 million was also imposed on Amazon for a similar breach.

According to an economist at the Chambers of Commerce and Industry, compliance costs for small and medium-sized enterprises (SMEs) associated with GDPR compliant data storage, processing and transfer systems can vary between €20,000 and €50,000.[10] The pay-offs are seen as reputational: compliance with GDPR engenders trust on the part of consumers.

The Law for a Digital Republic came into force in October 2016. It promotes an open data concept. In particular, it mandates public bodies and businesses undertaking public services to publish data in an anonymised format. The particular aim is to facilitate innovation and start-ups by making data available to these

France is also one of the major drivers of the GAIA-X initiative, which seeks to establish a common data infrastructure across the EU single market and develop a pan-EU cloud ecosystem. (Please also refer to the EU Deep Dive analysis).

[10] https://blogs.economie.gouv.fr/les-cafes-economiques-de-bercy/le-rgpd-une-bonne-nouvelle-pour-la-competitivite-des-entreprises/

Relationship to trade agreements

As a member of the EU, France delegates the competence for trade agreements to the European Commission, including on matters related to data and digital sectors. (Please refer to section on the EU Deep Dive).

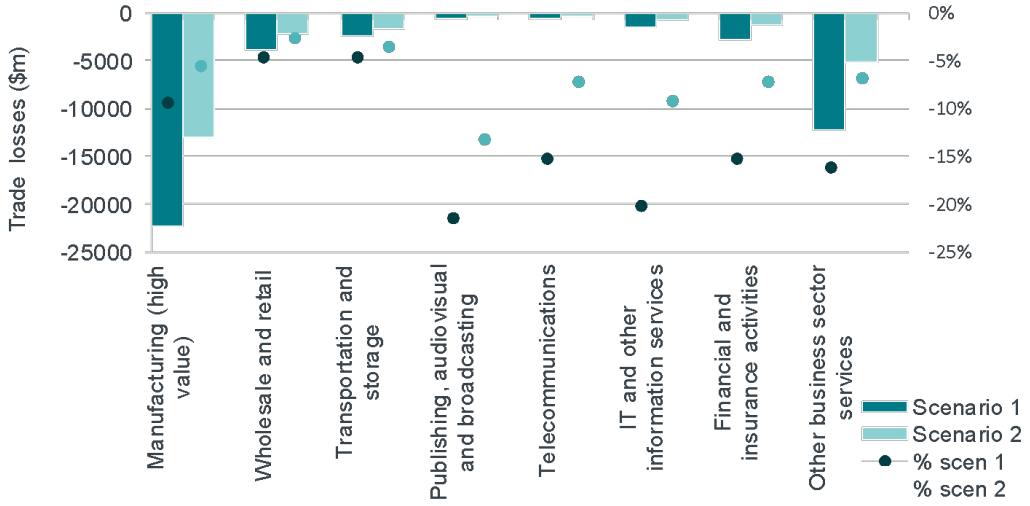
3.3.3 Impacts analysis

We analyse the impacts of data localisation by measuring how changes to restrictions on cross-border data flows affect the value of trade. We consider two scenarios.

- Scenario 1: Under this scenario, we assume France and its trade partners move from current practices to full data localisation. The difference captures the value at risk for France of losing current levels of international liberalisation and reverting to a restrictive international environment for data transfers.
- Scenario 2: Under this hypothetical scenario (as GDPR applies across all EU member states), starting from full restrictions on cross-border data flows, we assume France is considered adequate by the EU for GDPR purposes. From a French perspective, when compared to scenario 1, this captures the benefits of intra-EU data liberalisation in a context in which extra-EU data flows remain restricted.

The results are reported in Figure 13 below.

Figure 13 Trade impact analysis for France



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

Both France and its main trading partners are relatively liberalised, so the increased restrictiveness under scenario 1 generates significant impacts. In absolute terms, these effects are highest in high value-added manufacturing. Pronounced impact is observed particularly in other business services (including professional services). Cumulative scenario 1 impacts represent around 7% of France's exports. The results can also be interpreted as measuring the losses that could be avoided by trade agreements which help to secure existing levels of

liberalisation between France and its major trading partners (including EU partners).

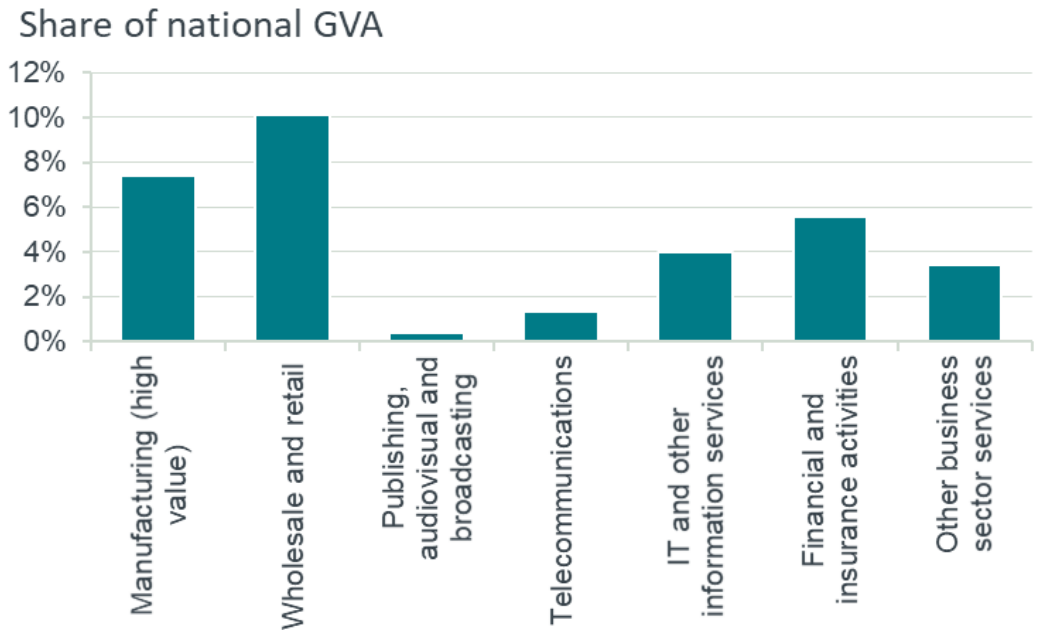
Under scenario 2, we in effect assume restrictions remain on extra-EU data flows but that intra-EU flows are liberalised through adequacy. For most sectors, and other business services specifically, this significantly reduces the losses reported under scenario 1. This reflects the importance of intra-EU trade and data flows to France and in turn underscores the value to France of securing an integrated architecture for data across the EU. The residual losses can be interpreted as the value to France of securing commitments from major non-EU trade partners of not rolling back current levels of liberalisation. In absolute terms, these residual losses still remain relatively substantial in high-value manufacturing, pointing to the value of these extra-EU negotiations to France.

3.4 India

3.4.1 Country background

Figure 14 shows the contribution of the data-intensive sectors to India's GVA. Collectively, the data-intensive sectors account for 32% of India's GVA. The most significant sector is wholesale and retail (10% of GVA), followed by high-value manufacturing (7%), and financial and insurance activities (6%).

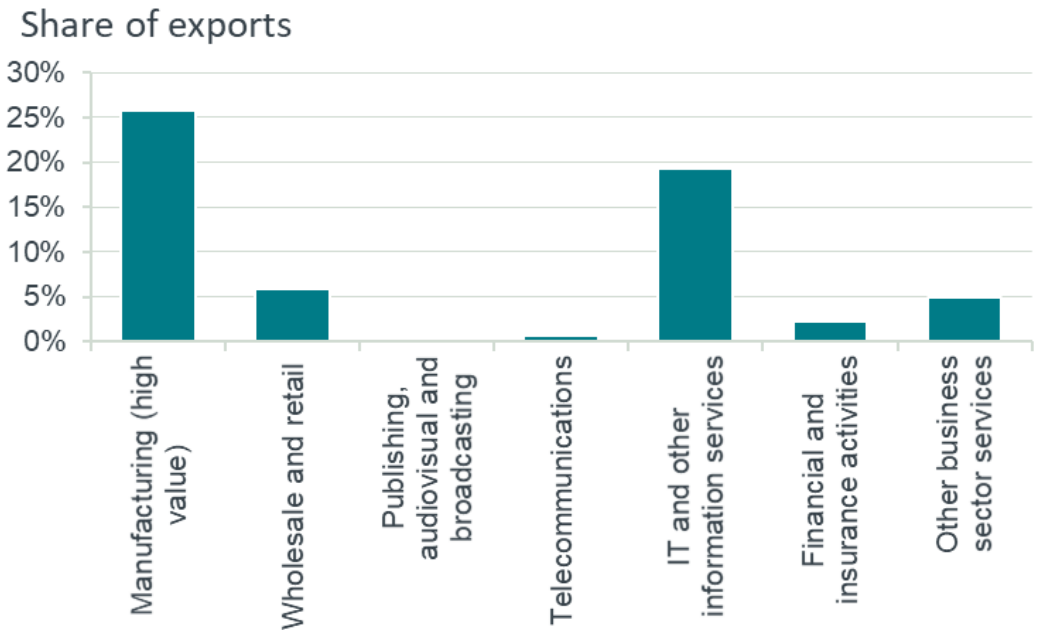
Figure 14 Share of India's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 15 shows each data-intensive sector's share of the value of exports from India. The data-intensive sectors account in total for 59% of the value of Indian exports. The two most significant data-intensive sectors are the high-value manufacturing sector and the IT and other information services sector; they respectively account for 26% and 19% of exports from India.

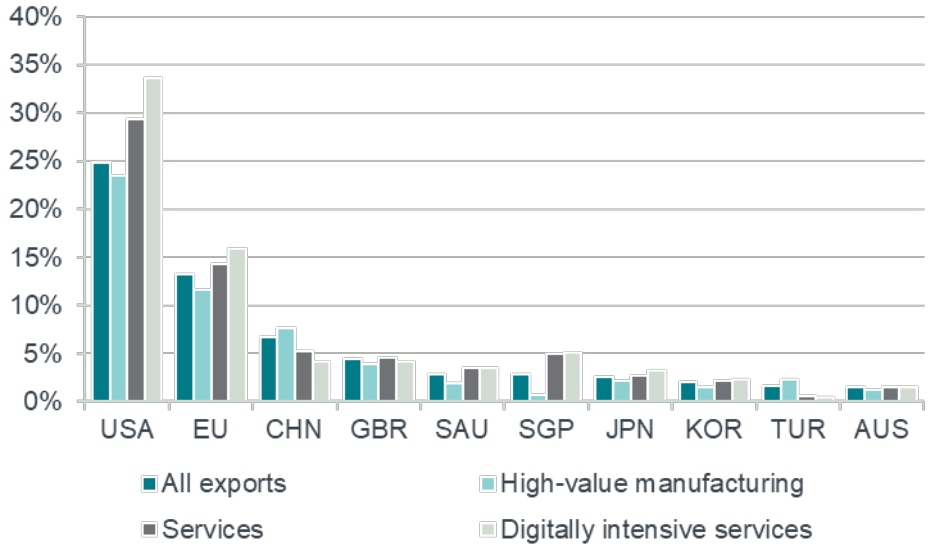
Figure 15 Share of India's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 16 shows that the UK is one of India's largest trading partners. Only the USA, the EU and China trade more with India than the UK does. The USA is India's largest trading partner with respect to digitally intensive services (receiving 34% of exports). The USA is followed by the EU (a 16% share of digital-intensive services exports), Singapore (5%) and then the UK (4%).

Figure 16 India's ten largest trading partners (percentage share of exports by country by major category of exports)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.4.2 Domestic legal and policy framework

Current legislation

India has not yet enacted specific legislation on personal data protection, although (as discussed below) a draft data protection bill has been published. Despite the lack of specific legislation, other legal instruments set out some rights and rules concerning personal data. First, an amendment to the Information Technology Act (2000) introduces a right to compensation for the improper disclosure of personal information. Second, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Rules") impose requirements on the collection and disclosure of sensitive personal data in the private sector. Sensitive personal data include passwords; financial information; physical, physiological and mental health condition; sexual orientation; medical records and history and biometric information.

The cross-border transfer of information that is not sensitive personal information is not subject to any restriction under the Rules. The Rules permit the transfer of sensitive personal information if the same levels of data protection are adhered to, provided that the data subject consents to the transfer or the transfer is necessary for the performance of a contract between the data subject and the transferor.

Proposed legislation

In August 2017, the Supreme Court of India delivered a landmark judgement recognising that the right to privacy is a fundamental right under the Indian constitution. The judgement imposed a positive obligation on the government to introduce legislation to enforce the right to privacy of individuals. Therefore, the Ministry of Electronics and Information Technology formed a committee in 2017 to formulate data protection rules. The committee issued a draft Personal Data Protection Bill, 2018, which – after deliberations – was tabled in the lower house of the Indian parliament as the Personal Data Protection Bill, 2019. It is unclear when the bill will be put to a vote.

The bill allows the government to classify instances of personal data as "critical personal data" which must not be transferred outside of India. The bill also requires a copy of all "sensitive personal data" that is transferred outside of India to be retained in the country. As extensive as the localisation requirements are in the bill, the localisation requirements in the 2018 draft of the bill were much more extensive. The 2018 draft mandated that a live copy of all personal data must be stored in India.

The bill allows sensitive personal data to be transferred outside of India, with the consent of the data subject, if the transfer is: made in accordance with contractual clauses or intra-group schemes authorised by the regulator; or made to a country, sector within a country, or international organisation approved by the government; or is deemed necessary by the regulator.

In stark contrast to the strict explicit restrictions on cross-border transfers of sensitive and critical personal data, the bill does not contain specific provisions on the cross-border transfer of non-sensitive, non-critical personal data. It is probable

that the cross-border transfer of such data will be subject to the general requirements for the lawful processing of personal data.

Sectoral requirements

In April 2018, the Royal Bank of India issued a (one-page) directive requiring all payment system providers to ensure that the "entire data relating to payment systems operated by them are stored in a system only in India". Providers were given six months to implement this measure and were also required to submit an audit report confirming their compliance. The directive states that the localisation of payment data was necessary to achieve "better monitoring". Localisation, the directive said, "would allow unfettered supervisory access to data".[11]

Balancing trade benefits with other public policy objectives

The data governance framework described in the draft Personal Data Protection Bill would cause some significant obstacles to trade. For example, the bill would require a copy of personal financial data (and other forms of sensitive personal data) to be stored in India.

It could be argued then that the bill was drafted with greater concern for certain public policy objectives at the expense of realising the benefits of trade to their fullest extent. Recall that the draft bill was proposed as a direct consequence of a Supreme Court ruling that Indian citizens have a right to privacy, including informational privacy. An expert committee report accompanying the draft bill argues that data localisation is necessary to limit foreign surveillance of Indian citizens.[12]

3.4.3 Modelling the impacts of data localisation

In this section, we estimate how changes to restrictions on cross-border data flows affect the value of India's trade under two scenarios.

In the first scenario, we assume that India and its trading partners move from their current practices to full data localisation. This provides an estimate of the value at risk for the economies. This move to full localisation would be (largely) consistent with GATS, and so this analysis reflects the value of "locking in" current levels of liberalisation (for example, through a FTA).

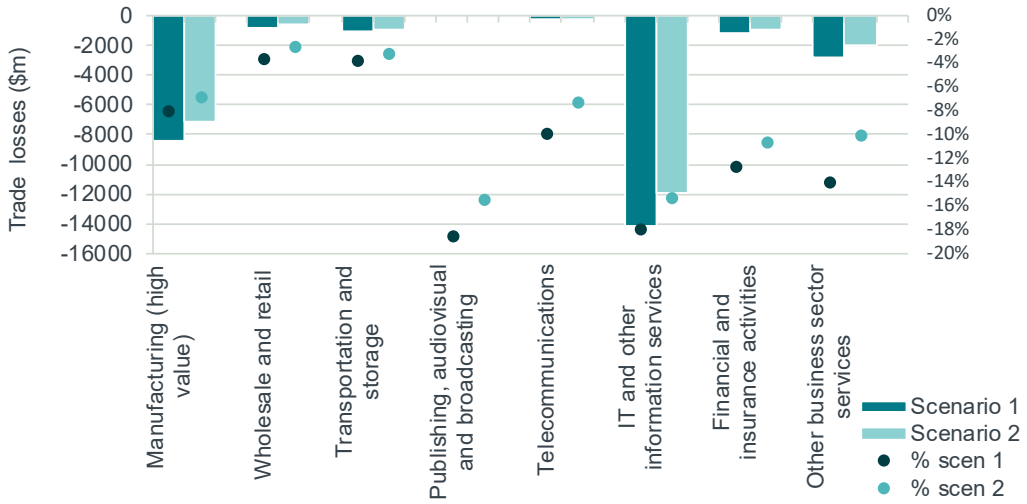
In the second scenario, we assume that India then moves from the full data localisation restriction situation under scenario 1 to agreeing reciprocal data arrangements with the EU.

Figure 17 below shows the trade losses for data-intensive service sectors from scenarios 1 and 2. The bars represent the absolute loss of trade (in $m, as measured by the left-hand vertical axis), and the dots represent the percentage loss of trade (as measured by the right-hand vertical axis).

[11] https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[12] Chapter 6, Section 2. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Figure 17 Trade impact of data localisation modelling results for India



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

The bulk of the trade losses from both scenario 1 and scenario 2 materialise from the IT and other information services sector. This sector accounts for a large proportion of India's trade (50% of trade in services and 20% of total trade). The percentage trade losses of the IT and other information services sector as a result of scenarios 1 and 2 are comparable to those of financial and insurance activities, publishing, audio-visual and broadcasting, and other business services. High-value manufacturing suffers substantial losses in absolute terms, and to some extent in relative terms, under both scenarios.

The results provide particular insights into the costs of data localisation for India. They fall heavily on sectors that are of key export interest and which Indian authorities have long targeted (with only moderate success) via industrial policy. The results suggest that initiatives to limit data localisation would have particularly significant pay-offs. They are telling insofar as they also shed light on the costs to India of its longstanding reluctance to engage on data and digital matters in trade negotiations. India is currently not party to the plurilateral negotiations underway at the WTO on data and digital matters, and it pulled out of the RCEP negotiations (for broader reasons than data matters), which could have provided it with a starting point for addressing data localisation at home and in partners.

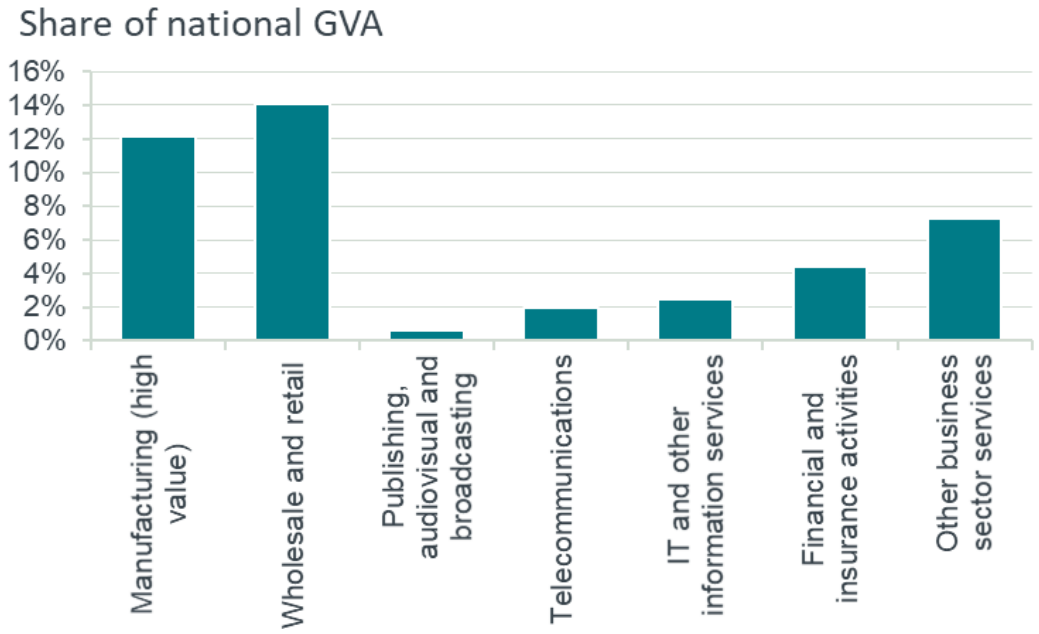
As the EU accounts for a relatively small share of India's trade, the impacts of scenarios 1 and 2 are not materially different. The impact of scenario 1, when measured across all service sectors, amounts to a trade loss equivalent to 5% of all trade. The small differences between scenarios 1 and 2 suggest that the priority for India would be to secure commitments from non-EU trade partners that they avoid roiling back on existing liberalisation commitments. This underscores the point made above about India's interest in reversing its longstanding recalcitrance in engaging with international negotiations on this subject.

3.5 Japan

3.5.1 Country background

Data-intensive sectors represent a significant proportion (43%) of Japanese GVA. Figure 18 below shows the share of GVA for each data-intensive sector. The largest data-intensive sector is wholesale and retail (representing 14% of Japanese GVA), followed closely by high-value manufacturing (12%). The five remaining data-intensive sectors each account for between 1% and 7% of Japanese GVA.

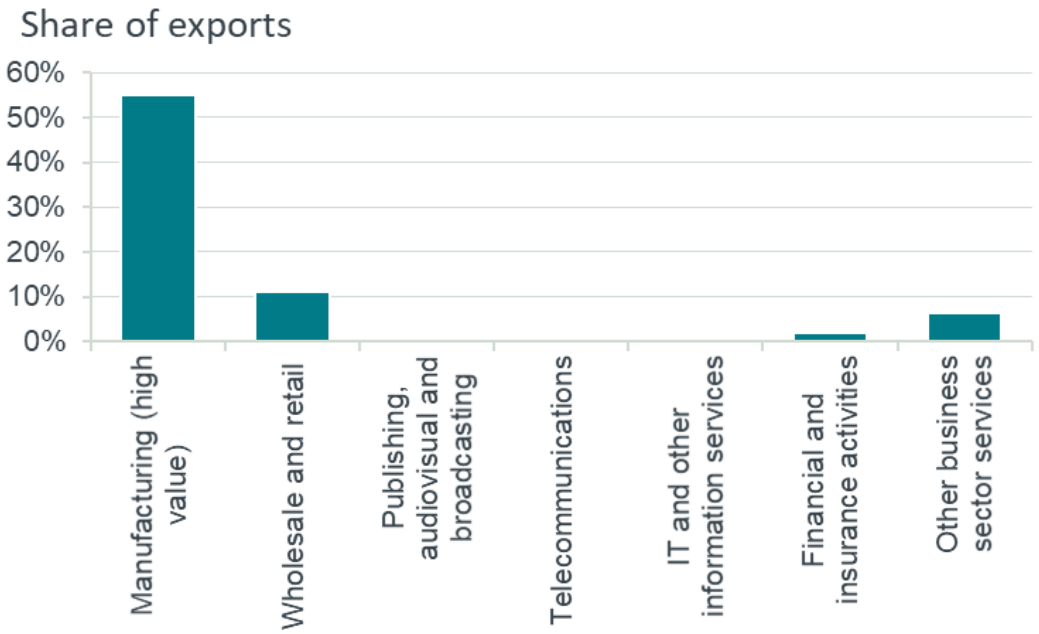
Figure 18 Share of Japan's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

The data-intensive sectors represent 75% of the value of Japanese exports. Figure 19 shows each data-intensive sector's share of Japanese exports. The most significant data-intensive sector in Japan by far is the high-value manufacturing sector; it accounts for 55% of exports from Japan. The wholesale and retail sector accounts for 6% of Japan's exports, while financial and insurance activities account for 2%. The other sectors do not represent a material share of Japanese exports.

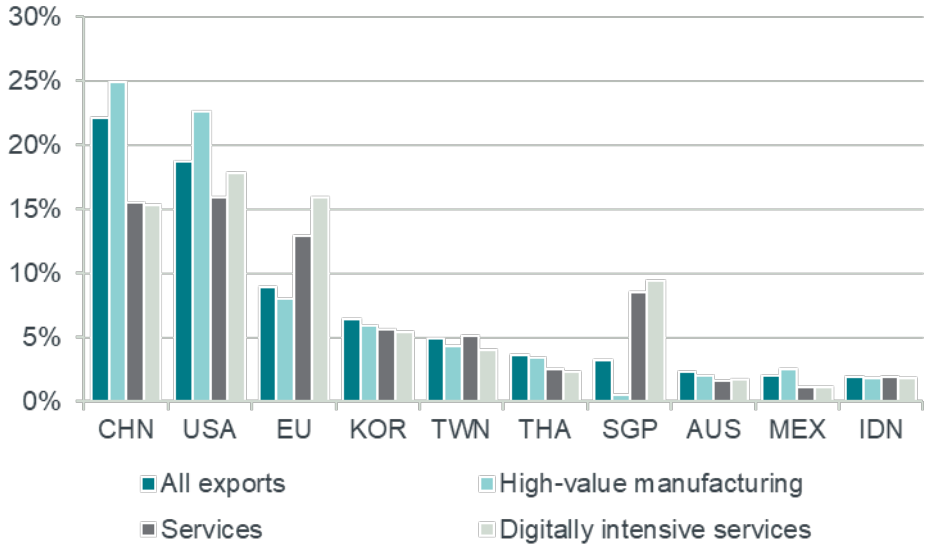
Figure 19 Share of Japan's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 20 shows Japan's ten largest trading partners. The three largest trading partners (in terms of the value of all exports) are China, then the USA and then the EU. The USA, EU and Singapore account for a disproportionate share of exports from digitally intensive service sectors (relative to their share of all exports). The Figure shows us that the UK is not among Japan's ten largest trading partners.

Figure 20 Japan's ten largest trading partners (percentage share of exports by country by major category of exports)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.5.2 Domestic legal and policy framework

Japan has a stringent personal data protection regime and is the subject of an adequacy decision from the European Commission. The key personal data protection legislation in Japan is The Act on the Protection of Personal Information ((APPI), Act No. 57 of 2003). The APPI was substantially amended in 2015 and the Amended APPI came into force from 2017. Under a provision of the Amended APPI, the government is required to review the APPI every three years.

The APPI defines personal information as information about a living person which either in its own right or in combination with other information reveals the identity of the individual.

The transfer of personal data to a third party in a foreign country is possible subject to the requirements of two mechanisms: the consent mechanism and the "opt-out" mechanism.

Under the consent mechanism, a transfer of personal data can be made if the data subject gives their consent. Their consent must be clear and cover the transfer to a third party in the foreign country. The data subject must be given the information necessary to judge whether to provide consent. The data subject must be informed about the level of protection afforded to personal data in the foreign country.

Under the opt-out mechanism, data subjects are notified about a proposed transfer of their personal information and given the opportunity to object. If a data subject does not exercise their opt-out right in a prescribed period then their personal information may be transferred. This mechanism can only be used to transfer data if the transfer is to a country deemed as having a data protection regime equivalent to the APPI or if the third party implements data protection standards equivalent to those prescribed by the APPI. The requirement for equivalent standards can be met if the third party is accredited under APEC's cross-border privacy rules system, if the third party is in the same corporate group, or the data controller and the third party enter into a contract.

Japan does not have any "absolute" data localisation requirements. However, information security guidelines issued to government agencies by The National Centre of Incident Readiness and Strategy for Cybersecurity state that in certain circumstances government information systems should be "isolated" from the internet.[13] This is by no means a blanket requirement but rather a measure which should be considered in light of the sensitivity of the data within the information system. This measure would indirectly lead to data localisation.

Balancing trade benefits with other public policy objectives

Japan's principal competing public policy objective is the protection of its citizens' data privacy rights. Japan has a robust data protection regime which freely permits cross-border personal data flows conditional on the ongoing protection of these rights. The GDPR framework is conceptually similar.

[13] Compliance Requirements. https://www.nisc.go.jp/eng/pdf/Common%20Standards(FY2016).pdf

3.5.3 Free trade agreements

Japan is a signatory to the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). The CPTPP requires signatories to "allow the cross-border transfer of information …, including personal information, when this activity is for the conduct of the business" (Article 14.11.2) and to not require businesses "to use or locate computing facilities in that [signatory's] territory as a condition for conducting business" (Article 14.13.2). These provisions imply greater liberation relative to the WTO baseline, but both provisions are subject to counterbalancing provisions. Japan has the scope to implement measures inconsistent with the above provisions to achieve a "legitimate public policy objective", provided that the measures would not constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade and the measures are not more restrictive than required to achieve the policy objective. The extent to which these conditions on the pursuit of legitimate public policy objectives create disciplines that limit the scope for discretionary policy interventions that restrict cross-border data flows remains to be tested.

Japan's FTA with the EU contains no specific provisions on cross-border data, other than a "rendez-vous clause" committing both parties to revisit the issue. In the event, the EU granted Japan adequacy status in 2020, and Japan reciprocated by considering the EU's data governance regime as equivalent to its own.

Separately, the UK-Japan Comprehensive Economic Partnership Agreement contains provisions concerning data localisation and cross-border data flows. Article 8.84(1) prohibits both countries from restricting cross-border data transfers needed for business purposes, and Article 8.85(1) requires both countries to not insist on the use of local computing facilities as a condition of conducting business in their country.

However, both measures are subject to counterbalancing measures. Article 8.84(2) allows either country to adopt or maintain restrictions on cross-border data flows to achieve a legitimate public policy objective, provided the measure is not a disguised restriction on trade nor a form of arbitrary or unjustifiable discrimination and does not impose restrictions greater than those required to achieve the objective. Article 8.85(2) allows either country to implement requirements on the use of local computing facilities that "are *necessary* to achieve a legitimate public policy objective", provided the requirements would not "constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade".

3.5.4 Modelling the impacts of data localisation

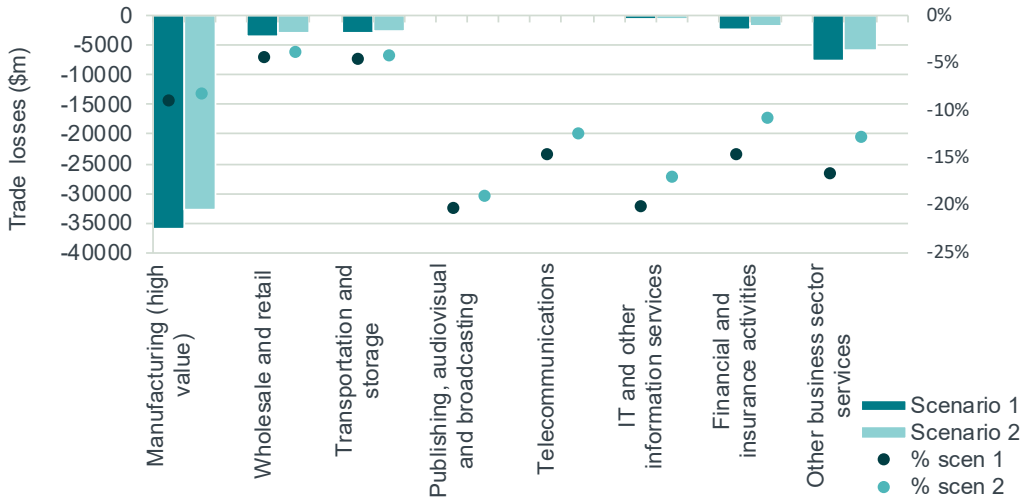
In this section, we estimate how changes to restrictions on cross-border data flows affect the value of Japan's trade under two scenarios.

In the first scenario, we assume that Japan and its trading partners move from their current practices to full data localisation. This provides an estimate of the value at risk for the economies. This move to full localisation would be (largely) consistent with GATS, and so this analysis reflects the value of "locking in" current levels of liberalisation (for example, through a FTA).

In the second scenario, we assume that Japan then moves from the full data restriction situation under scenario 1 to agreeing reciprocal data arrangements with the EU.

Figure 21 below shows the trade losses for data-intensive service sectors from scenarios 1 and 2. The bars represent the absolute loss of trade (in $m, as measured by the left-hand vertical axis), and the dots represent the percentage loss of trade (as measured by the right-hand vertical axis).

Figure 21 Trade impact of data localisation modelling results for Japan



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

Japan starts from a relatively liberal baseline, so the scenarios represent large impacts on trade in proportional terms.

Unsurprisingly, high-value manufacturing demonstrates large negative impacts in absolute terms. Of the more sensitive service sectors, other business services are the largest and hence drive the overall impact on trade in services. However, these sectors account for a relatively small share of Japan's exports, compared with manufacturing and "physical" services such as transport. We can see that wholesale and retail, transportation and storage are much less sensitive to the scenarios than the other sectors (as shown by the small percentage impacts for these sectors).

The impact on trade across all sectors from scenario 1 is equivalent to around 7% of total exports. As Japanese trade with the EU is fairly limited, the impact of scenarios 1 and 2 are fairly similar.

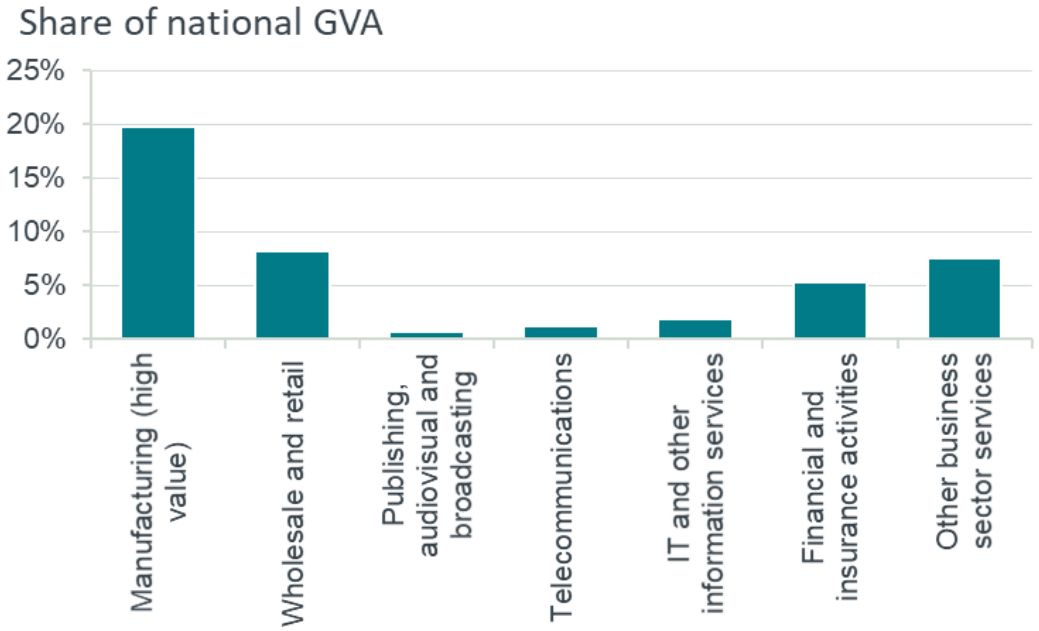
The losses from scenario 1 point to the value to Japan of securing commitments from partners, through FTAs for example, not to roll back from existing levels of liberalisation. The relatively small differences between scenarios 1 and 2 suggest that the priority for Japan lies in commitments from non-EU partners (e.g. through the CPTPP) to a greater extent than the adequacy agreement it has just secured with the EU.

3.6 South Korea

3.6.1 Country background

Figure 22 shows the contribution of the "data-intensive sectors" to South Korea's GVA. In total, these sectors represent 45% of South Korea's GVA. The most significant sector is high-value manufacturing, which accounts for 20% of South Korea's GVA. The wholesale and retail, financial and insurance activities, and other business services each account for 5% or more of GVA in South Korea.

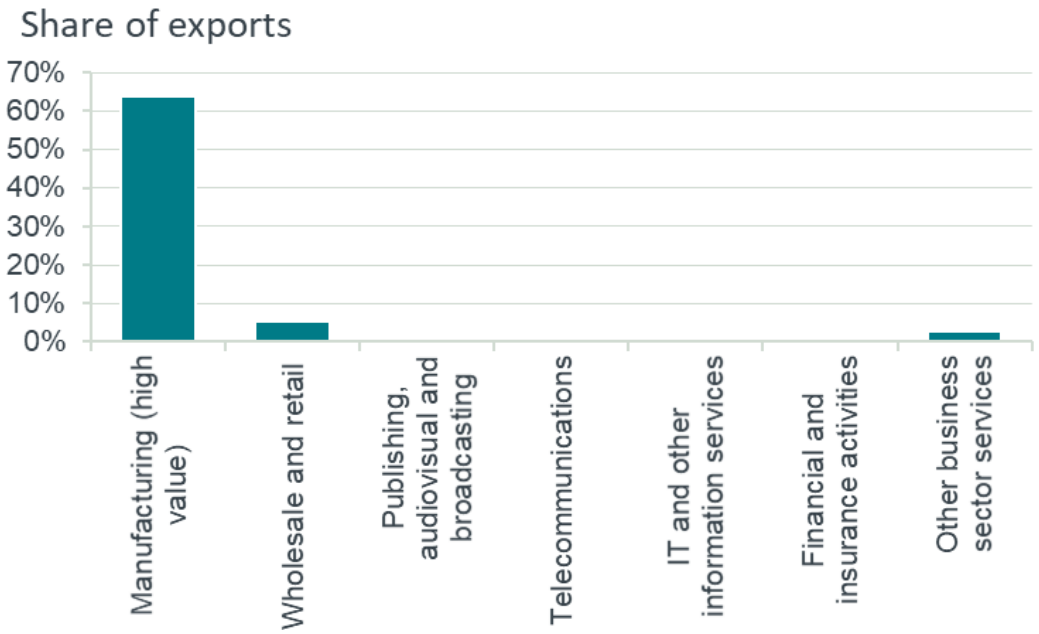
Figure 22 Share of South Korea's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Exports from the data-intensive sectors represent almost three-quarters (73%) of the total South Korean exports. Figure 23 shows each data-intensive sector's share of South Korean exports. The majority of exports from the data-intensive sectors come from the high-value manufacturing sector; 64% of the value of Korean exports come from this sector. The wholesale and retail, other business services, and financial and insurance activities sectors account for a small proportion of South Korean exports value.

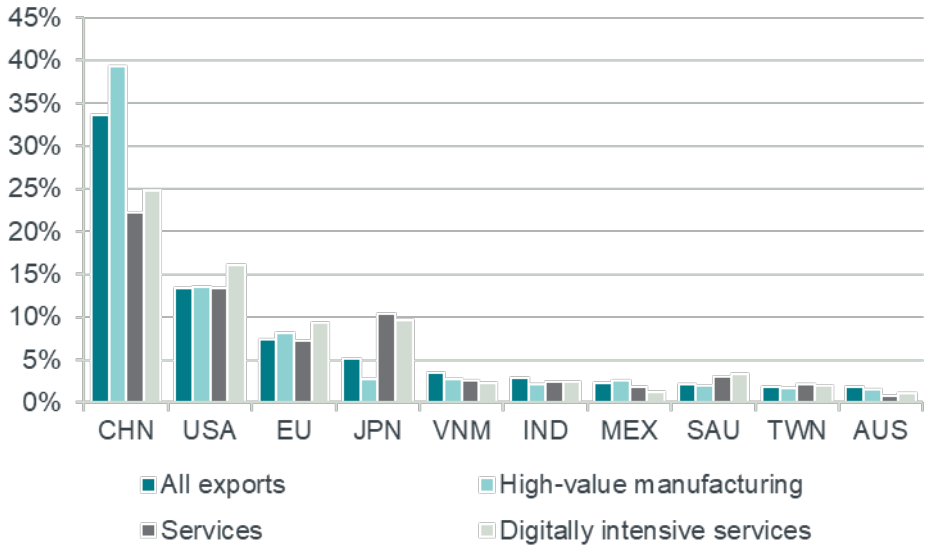
Figure 23 Share of South Korea's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 24 shows South Korea's ten largest trading partners. The three largest trading partners are China, the USA and the EU; they collectively account for 54% of South Korea's exports. While China is the largest consumer of South Korea's exports from digitally intensive service sectors, its share of digitally intensive service sector exports from South Korea is disproportionately small compared to its share of all exports.

Figure 24 South Korea's 10 largest trading partners (percentage share of exports by partner for export category)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.6.2 Domestic legal and policy framework

The main data protection law in South Korea is the Personal Information Protection Act (PIPA) which entered into force on 20 September 2011. However, PIPA was recently amended (effective from 5 August 2020). Other acts, related to the use of communication networks and credit information, themselves recently amended, also contain provisions governing the processing of personal information. The government has been pursuing an adequacy declaration from the European Commission. It is expected that the amendments to PIPA will clear the way for the European Commission to reach an adequacy decision.

PIPA defines personal information as any information pertaining to a living individual which identifies a specific person. This includes information which does not identify specific individuals by itself but which could identify specific individuals when combined with other information at reasonable cost and effort.

South Korea has been described as having one of the "strictest sets of data protection laws in the world",[14] so it may appear surprising that PIPA does not contain any specific rules on cross-border data transfers. PIPA regulates the transfer of personal data between a domestic data controller and a third party in the same fashion regardless of whether that third party is domestic or foreign. More specifically, PIPA requires data subjects to provide their explicit consent before their personal information is transferred to a third party. This means that consent is always required before personal data is transferred outside of South Korea. This can make the transfer of data more burdensome than otherwise, but it is not clear that this imposes a higher burden on cross-border transfers.

When seeking consent from the data subject, the transferor must inform the data subject of the recipient of the personal information; the purpose of use of personal information of the said recipient; the particulars of the personal information to be provided; the period when the personal information is retained and used by said recipient; the fact which data subjects are entitled to deny consent; and and disadvantage resulting from the denial of consent.[15]

South Korea has specific localisation requirements for spatial data. Under the Act on the Establishment, Management, etc. of Spatial Data (Act no. 12738, 3/6/2018), "no person shall take abroad maps, etc. or photos produced for the purpose of survey".[16] South Korea justifies this restriction on national security grounds; the country has a long history of closely guarding spatial data amid concerns about exposing sensitive information to North Korea (with which it is still technically at war).

South Korea also indirectly imposes a localisation requirement on public agencies. The Data Protection Standards for Cloud Computing Services Guidelines require providers of cloud computing services to public agencies to use data centres in

[14] One Trust. South Korea – Data Protection Overview. https://www.dataguidance.com/notes/south-korea-data-protection-overview

[15] Linklaters. Data Protected – Republic of Korea. https://www.linklaters.com/en/insights/data-protected/data-protected---republic-of-korea

[16] Article 16(1).

South Korea. While these guidelines are non-binding and there are no penalties for non-compliance, they are understood typically to be followed.[17]

Balancing trade benefits with other public policy objectives

South Korea's principal public policy objectives in the sphere of data are the protection of the data privacy rights of its citizens and national security. With regard to national security, South Korea's localisation requirements related to spatial data demonstrate a preference for ensuring national security objectives at the expense of the trade benefits forfeited. In terms of ensuring the data privacy rights of citizens, South Korea recognises the value of cross-border data flows, and allows such flows provided there is ongoing protection of their citizens' rights.

South Korea adopts relatively strict conditions on cross-border data flows. Namely, South Korea has stringent consent requirements, which means that all cross-border flows of personal data require the consent of data subjects. This is a potentially significant barrier to cross-border data flows.

3.6.3 Free trade agreements

South Korea is in the process of negotiating its accession to the CPTPP. Should this be successful, it would commit to an agreement that includes a positive obligation to allow cross-border data flows for business purposes and a prohibition of requirements to use local computing facilities as a condition of doing business in a country.

Both obligations are subject to counterbalancing exceptions which would allow South Korea to implement contradictory measures to pursue legitimate public policy objectives provided that said measures are not a means of arbitrary or unjustified discrimination and a disguised restriction on trade, and not more restrictive than is required to achieve the policy objective. The agreement also recognises that each country has its own regulatory requirements concerning information transfer.

South Korea is also a signatory to the Regional and Comprehensive Economic Partnership (RCEP), which includes similar data flow/localisation liberalisation provisions as those in CPTPP. However, the RCEP's counterbalancing provisions make it difficult for parties to challenge each other's data localisation and transfer restrictions. RCEP allows parties to implement such restrictions if they are necessary to achieve public policy objectives. Importantly, the RCEP text explicitly states that it is for each party to determine for themselves what restrictions (if any) are necessary to achieve their own objectives.

South Korea's free trade agreements with the USA and the EU also include commitments to liberalise cross-border data flows (alongside counterbalancing clauses). These provisions are not as developed as the CPTPP provisions and are less likely to discipline South Korea's stance towards cross-border data flows.

[17] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

3.6.4 Modelling the impacts of data localisation

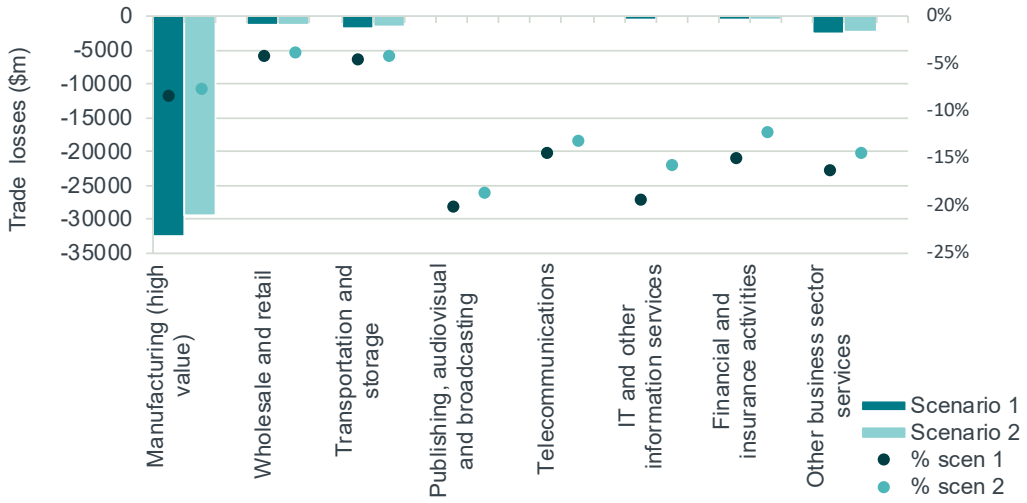
In this section, we estimate how changes to restrictions on cross-border data flows affect the value of South Korea's trade under two scenarios.

In the first scenario, we assume that South Korea and its trading partners move from their current practices to full data localisation. This provides an estimate of the value at risk for the economies. This move to full localisation would be (largely) consistent with GATS, and so this analysis reflects the value of "locking in" current levels of liberalisation (for example, through a FTA).

In the second scenario, we assume that South Korea then moves from the full data restriction situation under scenario 1 to agreeing reciprocal data arrangements with the EU.

Figure 25 below shows the trade losses for data-intensive service sectors from scenarios 1 and 2. The bars represent the absolute loss of trade (in $m, as measured by the left-hand vertical axis), and the dots represent the percentage loss of trade (as measured by the right-hand vertical axis).

Figure 25 Trade impact of data localisation modelling results for South Korea



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

The results of the trade modelling for South Korea are similar to those for Japan. Like Japan, South Korea starts from a liberal baseline, and so the percentage impacts of the two scenarios can be large.

As with Japan, high-value manufacturing is the most impacted sector, and both absolute and relative impacts are similar to those seen in Japan. We can see that wholesale and retail, and transportation and storage are much less sensitive to the scenarios than the other sectors (as shown by the relatively small percentage impacts for these sectors). Overall trade impacts are similar to Japan – around 7% in scenario 1.

Of the more sensitive service sectors, the other business services sector is the largest and drives the overall impact of the scenarios on trade in services. But, as South Korea's economy is weighted heavily towards manufacturing, service sectors account only for a small proportion of exports. As such, the impact on trade

across all service sectors of scenario 1 is equivalent to 1% of exports. Low trade with the EU means that the impact of scenario 2 is similar to that of scenario 1.

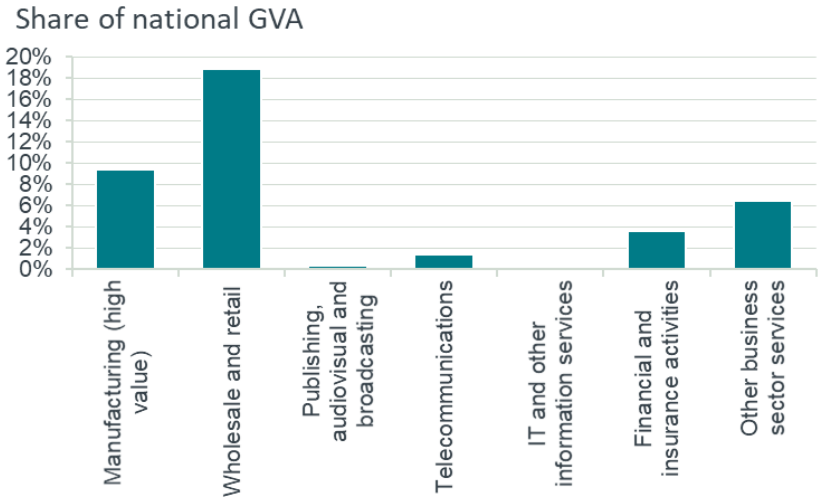
The results suggest that the priority for South Korea is to secure commitments from non-EU trade partners not to roll back from existing levels of liberalisation. South Korea is not yet a member of the CPTPP, and accession to it could be one vehicle for achieving this degree of security.

3.7 Mexico

3.7.1 Country background

The data-intensive sectors in Mexico together account for over 40% of the national GVA. As illustrated in Figure 26 below, the wholesale and retail sector accounts for 19%, followed by manufacturing at 10% of the national GVA.

Figure 26 Share of Mexico's GVA by data-intensive sector

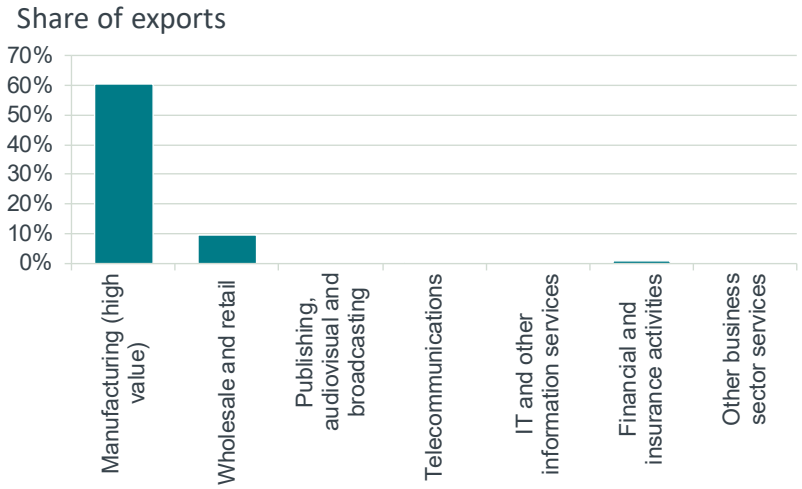


Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.

Note: Data refer to 2015.

These sectors together represent over 70% of total Mexican exports. This is illustrated in Figure 27. Notably, as much as 60% of the exports come from the manufacturing sector. The wholesale sector makes up close to 10% of exports, with the remaining sectors together accounting for less than 2%.

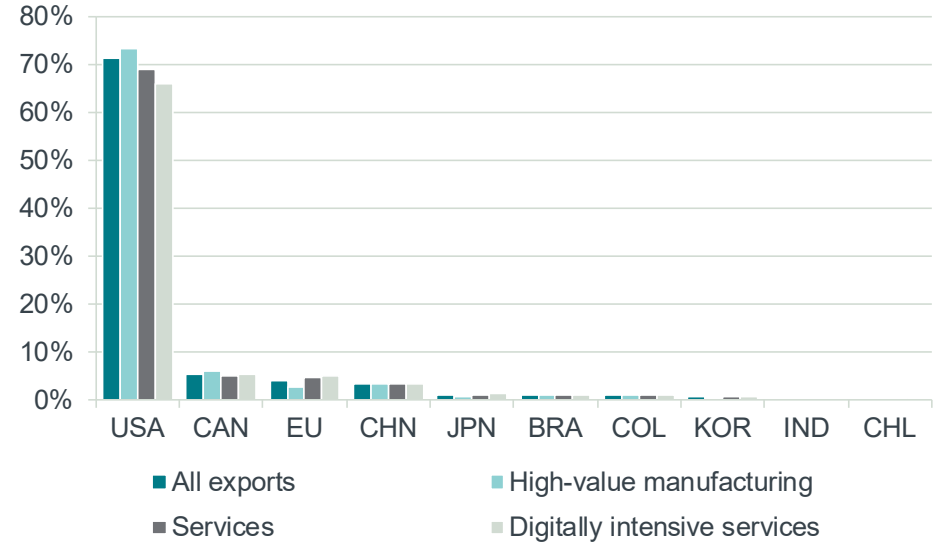
Figure 27 Share of Mexico's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 28 represents the top ten trading partners for Mexico. The USA is Mexico's main trading partner – accounting for over 70% of total exports. Significantly, it also contributes to close to 70% of services and 66% of exports from digitally intensive services. Shares of the other trading partners are considerably smaller: Canada, the EU and China together account for c. 13% of exports, while the remainder together account for c. 5%.

Figure 28 Mexico's ten largest trading partners (percentage share by partner for export category)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.7.2 Domestic legal and policy framework

The general data protection regulations in Mexico are defined by the Federal Law for the Protection of Personal Data in the Possession of Private Parties (LFPDPPP, in its Castilian acronym) supplemented by the Rules of the Federal Law for the Protection of Personal Data in the Possession of Private Parties (the "Regulation"). The law came into effect in 2010 and the Regulation came into effect in 2011.[18]

The LFPDPPP (as amended and supplemented by regulation) does not allow data to be transferred to countries offering adequate protections without the subjects' consent. Data may be transferred if the transfer and its purpose are stated in the relevant privacy notice and the subject gives their informed, prior consent to the notice.

Additionally, the data controller must provide third parties with the privacy notice that was sent to and consented to by the individual. Data processing must be consistent with what was agreed in the privacy notice, which will contain a clause indicating whether or not the data subject agrees to the transfer of their data. The third-party recipient assumes the same obligations as the data controller who has transferred the data.

The consent of the data subject is not required for a domestic or international transfer of personal data where the transfer is:

- Pursuant to a law or treaty to which Mexico is party;
- Necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;
- Made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies as the data controller;
- Necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject;
- Necessary or legally required to safeguard public interest or for the administration of justice;
- Necessary for the recognition, exercise or defence of a right in a judicial proceeding; or
- Necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject.

The Regulation establishes that consent by the data subject is not necessary for communications or transmissions of personal data to data processors. However, the data processor must do all of the following:

- Process personal data only according to the instructions of the data controller;

[18] https://www.linklaters.com/en/insights/data-protected/data-protected---mexico

- Not process personal data for a purpose other than as instructed by the data controller;
- Implement the security measures required by the Law, the Regulation and other applicable laws and regulations;
- Maintain the confidentiality of the personal data subject to processing;
- Delete personal data that were processed after the legal relationship with the data controller ends or when instructed by the data controller, unless there is a legal requirement for the preservation of the personal data; and
- Not transfer personal data unless instructed by the data controller, unless the communication arises from subcontracting, or if so required by a competent authority.

The local data protection laws are similar to the GDPR in some parts, such as the accountability principle and the Data Protection Impact Assessment, for which Mexico has a similar procedure.

Under Mexico's laws, it is not possible to transfer personal data to countries which offer adequate protection without additional contractual agreements.

Balancing freedom for cross-border data flows with public policy objectives

According to the Constitution of Mexico, the protection of personal data is a fundamental right of all Mexican citizens. In line with this, Mexico's data laws strongly defend the protection of personal information giving individuals the right to access, change, oppose or suppress their personal data.

Private companies must comply with these regulations or risk an administrative penalty (including significant sanctions) and may also be subject to civil liability. To some extent, therefore, the strong data protection rules may be seen as a barrier to trade flows and benefits that would be enjoyed under a less restrictive data protection regime.

3.7.3 Free trade agreements

As discussed in the previous section, Mexico has strong data protection rules in place for personal data, as defined under the LFPDPPP and supplemented by the Regulation.

In general, data protection regulations including data localisation measures are becoming increasingly intertwined with trade agreements. Mexico's key trade agreements in place are the United States-Mexico-Canada Agreement (USMCA) and the CPTPP. Key features of this agreement relate to data protection and localisation, and the potential implication of these are outlined below.

United States-Mexico-Canada Agreement (USMCA)

The (USMCA) is the renegotiated North American Free Trade Agreement (NAFTA), a 25-year-old pact.

This agreement includes a number of key updates to NAFTA including a full chapter (Chapter 19) on digital trade.[19] This chapter prohibits tariffs on digital goods and discrimination against foreign suppliers of digital goods and services, and includes positive obligations to eliminate barriers to data flows:

- Article 19.11(1) requires an elimination of barriers to cross-border data flows.
- Article 19.11(2) prohibits use or location of computing facilities in the territory as a condition of business in that territory.

The USMCA also includes a number of counterbalancing provisions relating to data protection:

- Specific counterbalancing measures apply to 19.11(1), and there is allowance to adopt or maintain measures "necessary" for legitimate public policy requirements. However, notably, the prohibition of localisation of computing facilities is not explicitly counterbalanced.
- The agreement also includes a reference to APEC's cross-border privacy rules as a way of balancing cross-border flows with information requirements.
- General exceptions under Article 32.1 of the agreement provide for the application of GATS Article XIV.

Finally, it is useful to understand the effects relative to the GATS/ WTO baseline and implications for current policy settings in this context. The wording of prohibitions in this agreement points to significant strengthening of liberalisation vis a vis GATS baseline and current practices (notably in Mexico). The inclusion of necessity tests in the counterbalancing provisions also reduces scope for discretionary localisation requirements.

Overall, while it is important to remember that Mexico has comprehensive data privacy and protection laws which companies doing business with Mexico must adhere to, the USMCA does take several steps to ease cross-border transfers of data between the USA, Canada and Mexico.

Notably this appears more closely aligned to the USA's approach of minimising data flow restrictions than to Mexico's relatively more restrictive approach to data protection. If applied, therefore, the USMCA provisions could significantly reduce the scope for Mexico to introduce data localisation in respect of the USA and Canada.

CPTPP

As discussed in section 3.5.3 on Japan, the CPTPP includes a positive obligation to allow cross-border data flows for business purposes and a prohibition of requirements to use local computing facilities as a condition of doing business in a country.

Both obligations are subject to counterbalancing exceptions which would allow Mexico to implement measures to pursue legitimate public policy objectives provided that said measures are not a means of arbitrary or unjustified

[19] USMCA, "Digital Trade" Chapter 19, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

discrimination and a disguised restriction on trade, and not more restrictive than is required to achieve the policy objective. The agreement also recognises that each country has its own regulatory requirements concerning information transfer.

3.7.4 Modelling the impacts of data localisation

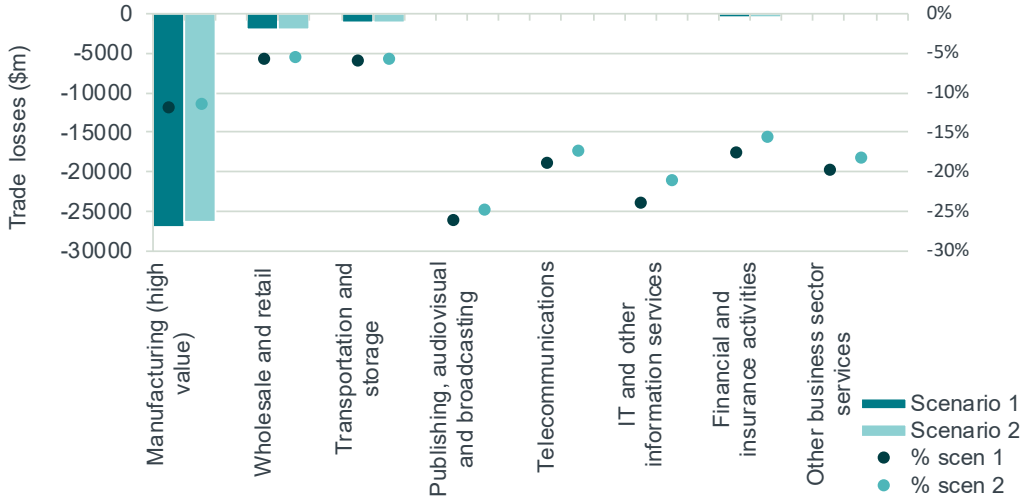
In this section, we estimate how changes to restrictions on cross-border data flows affect the value of Mexico's trade under two scenarios.

In the first scenario, we assume that Mexico and its trading partners move from their current practices to full data localisation. This provides an estimate of the value at risk for the economies. This move to full localisation would be (largely) consistent with GATS, and so this analysis reflects the value of "locking in" current levels of liberalisation (for example, through a FTA).

In the second scenario, we assume that Mexico then moves from the full data restriction situation under scenario 1 to agreeing reciprocal data arrangements with the EU.

Figure 29 below shows the trade losses for data-intensive service sectors from scenarios 1 and 2. The bars represent the absolute loss of trade (in $m, as measured by the left-hand vertical axis), and the dots represent the percentage loss of trade (as measured by the right-hand vertical axis).

Figure 29 Trade impact of data localisation modelling results for Mexico



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

Mexico has relatively few restrictions on data. The bulk of its trading partners, particularly the USA, also have liberalised regimes on cross-border trade. Consequently, the impacts of scenario 1 are among the highest observed across the countries studied in sectoral/percentage terms.

The bulk of Mexico's exports are accounted for by manufacturing, which explains the fact that this sector displays by far the biggest losses in absolute terms. Similarly to China, services represent a very limited proportion of exports and are heavily weighted towards wholesale and retail and transportation. Overall impacts on trade are in the order of 8% under scenario 1.

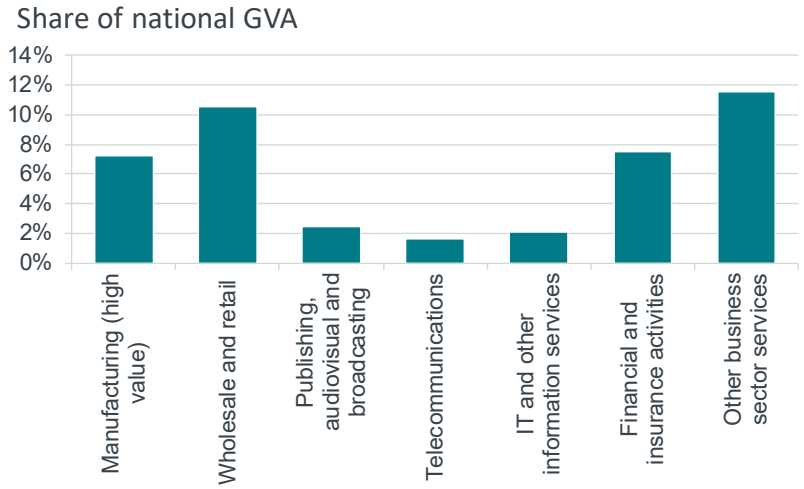
Low trade with the EU means that scenario 2 has little impact on exports, underscoring the value of agreements with other parties. On this front, Mexico is party to two agreements – USMCA and CPTPP – which have substantive provisions mandating the free cross-border flows of data. Of the two, the provisions of the USMCA are stronger. The results underscore the value of these provisions – both in terms of limiting the extent to which Mexico might be able to pursue data localisation efforts and thereby hinder its own exports and the extent to which partners (specifically the USA, which dominates Mexico's trade) could also take action that adversely impacts Mexico's trade prospects.

3.8 USA

3.8.1 Country background

The data-intensive sectors in the USA together account for over 40% of the national GVA. As illustrated in Figure 30 below, the wholesale and retail sector accounts for 11%, with financial services and manufacturing accounting for 8% and 7% respectively.

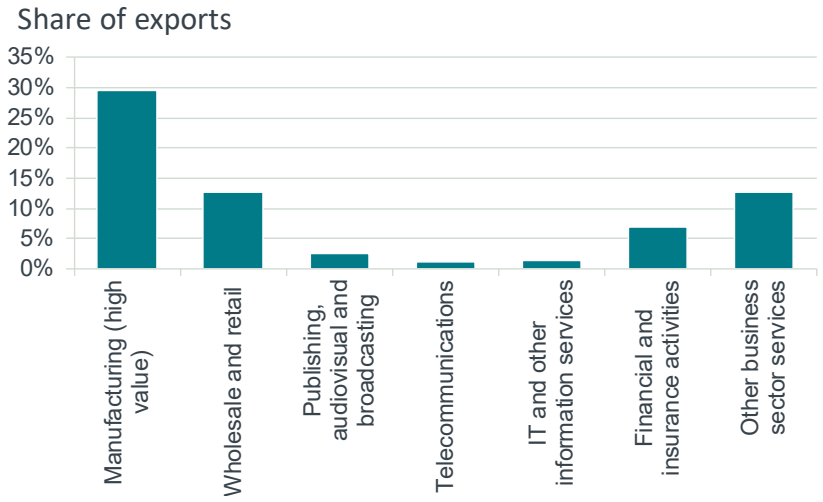
Figure 30 Share of USA's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Figures are for the year 2015.

These sectors together represent close to 70% of total US exports. This is illustrated in Figure 31. Thirty percent of the exports come from the manufacturing sector – more than double the contribution of any of the other sectors. The wholesale and retail sector and other business services have similar shares at c. 13% each, while financial and insurance activities contribute to 7% of overall exports.

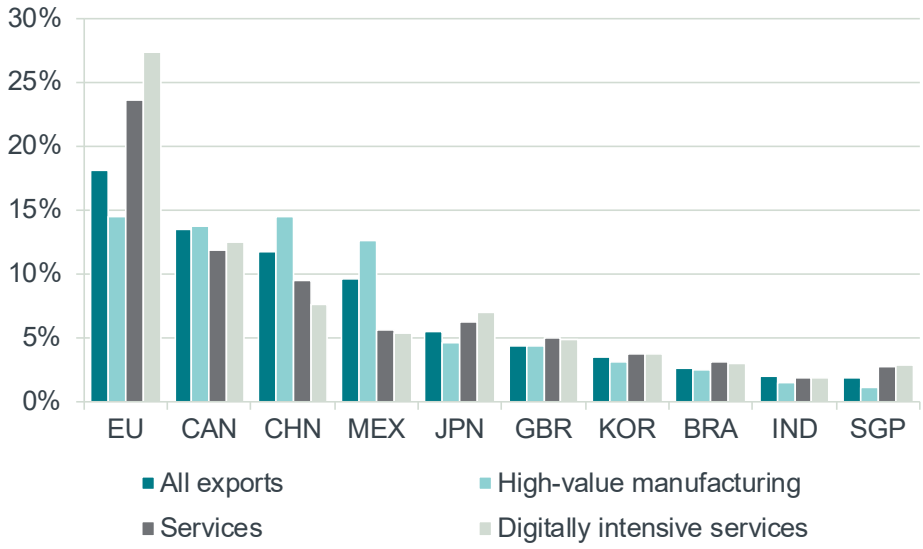
Figure 31 Share of USA's exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 32 represents the top ten trading partners for the USA. The three largest trading partners – EU, Canada and China – together account for over 40% of US exports. The EU is the USA's largest trading partner, accounting for close to 20% of all US exports. Significantly, it also contributes to 24% of services and 27% of exports from digitally intensive services – more than double the contribution of the other trading partners.

Figure 32 Top ten trading partners for the USA (percentage share of exports by country by major category of exports)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

3.8.2 Domestic legal and policy framework

The USA's stance has broadly been against data localisation laws, arguing that they unnecessarily impair electronic commerce and could, in fact, harm the

economies of countries that adopt them. According to a United States International Trade Commission (USITC) report, data localisation measures and specific laws pertaining to the flow of data have forced companies to leave specific markets and could impede the development of information technology.[20]

There is no national law on data privacy in the USA and few limits on the transfer of personal data outside the USA, but the entities exporting it remain liable in case of misuse.

State-level privacy laws are common, and several states have enacted laws that limit or discourage state agencies or state contractors from outsourcing data processing beyond US borders. However, these laws are typically limited to state government agencies and private companies that contract to perform services for or provide goods to state agencies.

California Consumer Privacy Act

Notably, California was one of the first states to provide an express right of privacy in its constitution and was also the first to pass a data breach notification law. This was followed by the California Consumer Privacy Act (CCPA) of 2018, the nation's first state-wide data privacy law, which applies to all firms established in the state.

According to this act, firms must give consumers the opportunity to learn of the categories of personal information that they collect, sell or disclose about them, and to whom the information is sold or disclosed. The act also gives consumers the right to prevent businesses from selling or disclosing their personal information. Individuals must therefore be informed that their information may be sold and that they have a "right to opt out".

Overall, however, governance and requirements on data privacy and data protection in the USA are significantly less restrictive compared other regimes, and specifically do not include restrictions on the cross-border transfer of personal data.

The CLOUD Act

Another relevant area to consider around US regulation relating to data localisation is the role and powers of the US government to obtain data, even if it is outside the USA. The US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) passed in 2018 gives US law enforcement authorities the power to request data stored by businesses established in the USA (which includes most major cloud providers) even if it is **outside the USA**. This act has two main provisions:

- It allows US law enforcement to access electronically stored communications data located outside the USA provided that the information sought is relevant and material to an ongoing criminal investigation.
- It creates a framework within which the USA can enter into bilateral (or executive) agreements with foreign states.

Importantly, this act does not impose new obligations on US or foreign communications service providers and is also balanced by a number of safeguards

[20] Coffin, David. "Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions". USITC, 2017. https://www.usitc.gov/publications/332/pub4716_0.pdf

intended to prevent abuse. However, where personal data is stored in the EU, this may conflict with the GDPR.[21]

Balancing freedom for cross-border data flows with public policy objectives

US trade policy reflects the growing importance of data flows and digital economic activity. As a leader in e-commerce, the USA houses some of the most globally competitive suppliers of digital goods and services. For instance, four US companies – Amazon, Microsoft, Google and IBM – are the leading providers of cloud computing services in the world.[22] Beyond the global reach of these large companies, many smaller innovative service providers and local, small businesses are able to leverage an online presence to provide services around the globe.

The US data governance framework and objectives are in line with broader policy objectives to minimise trade barriers for e-commerce and more traditional industries, and they protect and advance the development of information technology.

3.8.3 Free trade agreements

As discussed in the previous section, the USA supports eliminating as many barriers to data flows as possible and views data localisation laws as another barrier to trade. Data localisation measures are becoming increasingly intertwined with trade agreements. The USA has typically sought to ban data localisation requirements in modern trade agreements. Key trade agreements in which the USA is involved and the potential implications of these are outlined below.

United States-Mexico-Canada Agreement (USMCA)

The USMCA is the renegotiated North American Free Trade Agreement (NAFTA), a 25-year-old pact. In line with the broader US objective to minimise data localisation measures, this was the first US trade agreement to incorporate a data localisation ban.

This agreement includes a number of key updates to NAFTA including a full chapter (Chapter 19) on digital trade.[23] This chapter prohibits tariffs on digital goods and discrimination against foreign suppliers of digital goods and services, and includes positive obligations to eliminate barriers to data flows:

- Article 19.11(1) requires an elimination of barriers to cross-border data flows.
- Article 19.11(2) prohibits use or location of computing facilities in the territory as a condition of business in that territory.

According to the U.S. International Trade Commission (ITC), "protection from localization laws is essential for U.S. carriers seeking to manage data processing and network management functions from a centralized location". In estimating USMCA's economic impact on the USA, the ITC notes that "USMCA's Digital Trade

[21] https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe

[22] US International Trade Commission, "Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions", Aug 2017. https://www.usitc.gov/publications/332/pub4716_0.pdf

[23] USMCA, "Digital Trade" Chapter 19.
https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

chapter, along with provisions related to investment and e-commerce, contribute significantly to the model's estimated 0.17 percent increase in U.S. services sector output and 1.2 percent increase in services exports to the world".[24]

The USMCA also includes a number of counterbalancing provisions relating to data protection:

- Specific counterbalancing measures apply to 19.11(1), and there is an allowance to adopt or maintain measures "necessary" for legitimate public policy requirements. However, notably, the prohibition of localisation of computing facilities is not explicitly counterbalanced. The inclusion of an explicit necessity test reduces the scope of discretion in enacting a policy measure, as it allows a partner to challenge the grounds for the measure. This discipline is arguably more constraining than equivalent counterbalancing requirements in the CPTPP and RCEP agreements.
- The agreement also includes a reference to APEC's cross-border privacy rules as a way of balancing cross-border flows with information requirements.
- General exceptions under Article 32.1 of the agreement provide for the application of GATS Article XIV.

Finally, it is useful to understand the effects relative to the GATS/WTO baseline and implications for current policy settings in this context. The wording of prohibitions in this agreement points to significant strengthening of liberalisation vis a vis the GATS baseline and current practices (notably in Mexico). The inclusion of necessity tests in the counterbalancing provisions also reduces the scope for discretionary localisation requirements.

US-Korea

The US-Korea trade agreement was signed in September 2018, pledging to "refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders".
This agreement also includes general exemptions along the lines of GATS Article XIV(c). Overall, this points to a modest increase in disciplines on data localisation relative to the GATS baseline, with scope for discretion still maintained.

Others

The USA currently has trade agreements in force with twenty countries,[25] in addition to a number of agreements currently in negotiation. The terms of the US-Singapore trade agreement, for instance, are similar to the US-Korea agreement summarised above. US-EU and US-Kenya trade deals are currently in negotiation. It is understood that the USA is looking to include data localisation bans in both these agreements.[26]

[24] US International Trade Commission, "U.S.-Mexico-Canada Trade Agreement: Likely Impact on the U.S. Economy and on Specific Industry Sectors", April 2019. https://www.usitc.gov/publications/332/pub4889.pdf

[25] https://www.state.gov/trade-agreements/

[26] https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/

3.8.4 Modelling the impacts of data localisation

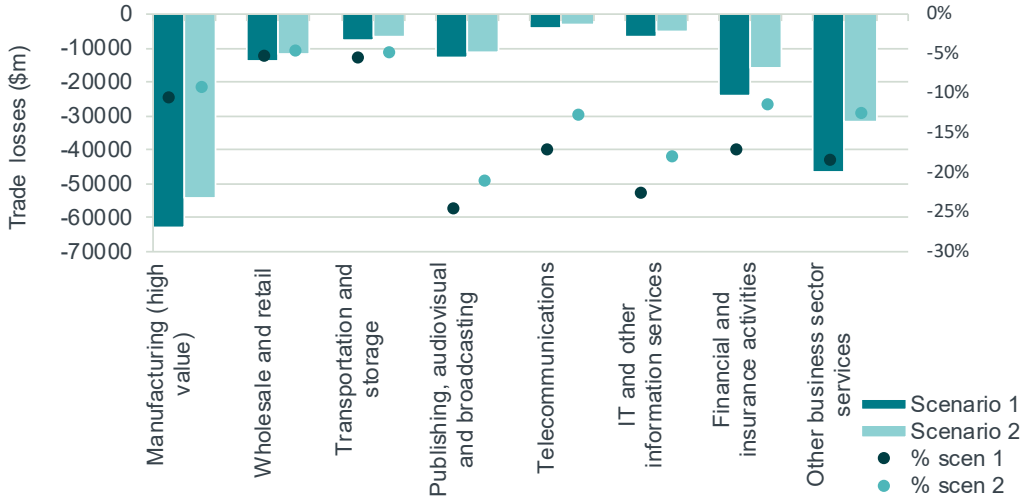
In this section, we estimate how changes to restrictions on cross-border data flows affect the value of the USA's trade under two scenarios.

In the first scenario, we assume that the USA and its trading partners move from their current practices to full data localisation. This provides an estimate of the value at risk for the economies. This move to full localisation would be (largely) consistent with GATS, and so this analysis reflects the value of "locking in" current levels of liberalisation (for example, through a FTA).

In the second scenario, we assume that the US then moves from the full data restriction situation under scenario 1 to agreeing reciprocal data arrangements with the EU.

Figure 33 below shows the trade losses for data-intensive service sectors from scenarios 1 and 2.

Figure 33 Trade impact of data localisation modelling results for USA



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

The USA's highly liberalised starting position means that US sectors are heavily affected by restrictiveness as represented by scenario 1. High-value manufacturing suffers the largest impacts in absolute terms. Of the services sectors, business and financial services stand out. The absolute value of impacts in these sectors is much larger than seen in other countries, reflecting the size of US-based businesses in the global trade of these sectors. Relative effects are also high and comparable to effects in many of the other countries.

In contrast, the wholesale and retail, transportation and storage sectors are much less sensitive to the scenarios than the other sectors (as shown by the relatively small percentage impacts for these sectors).

Under scenario 2, some of the losses reported under scenario 1 are attenuated. This is notably the case for financial services and other business services. They show the value at risk for specific sectors of losing free flow of personal data to the EU because of the rescinding of instruments such as the EU-US privacy shield. At the same time, residual losses under scenario 2 remain relatively large against those under scenario 1, suggesting that the priority for the USA is to enter into

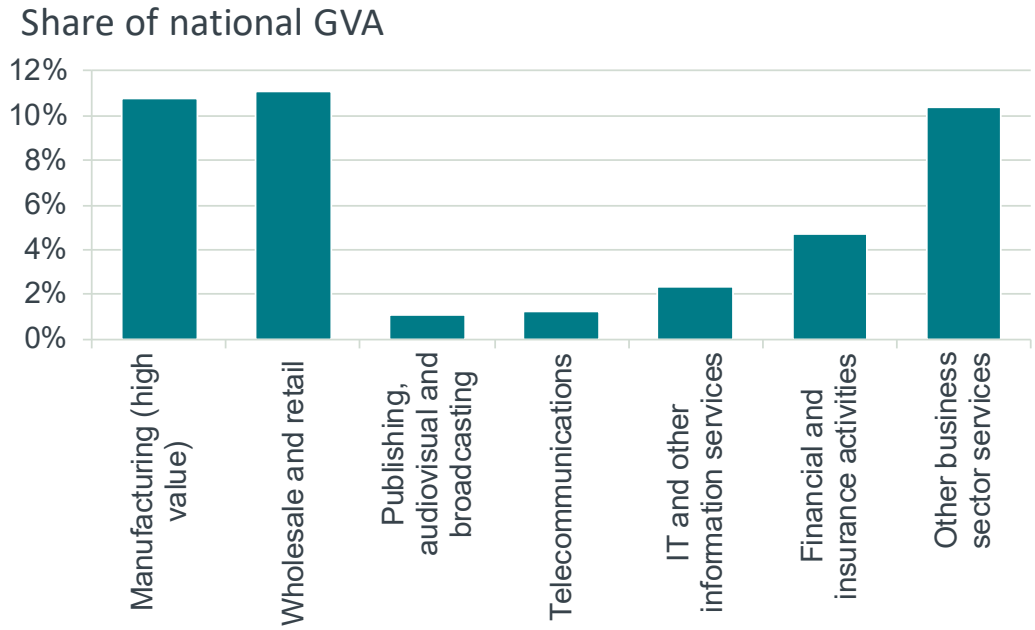
commitments with non-EU partners that provide safeguards against policy rollback. This explains the USA's determination to include strong data provisions in agreements such as the USMCA. It also underscores the potential value to the USA of acceding to the CPTPP (having pulled out of its predecessor, the Trans-Pacific Partnership).

3.9 European Union

3.9.1 Country background

Figure 34 shows the contributions of data-intensive sectors to EU GVA. Collectively, they account for just over 40% of GVA. Three sectors dominate: high value-added manufacturing, wholesale and retail manufacturing, and other business services.

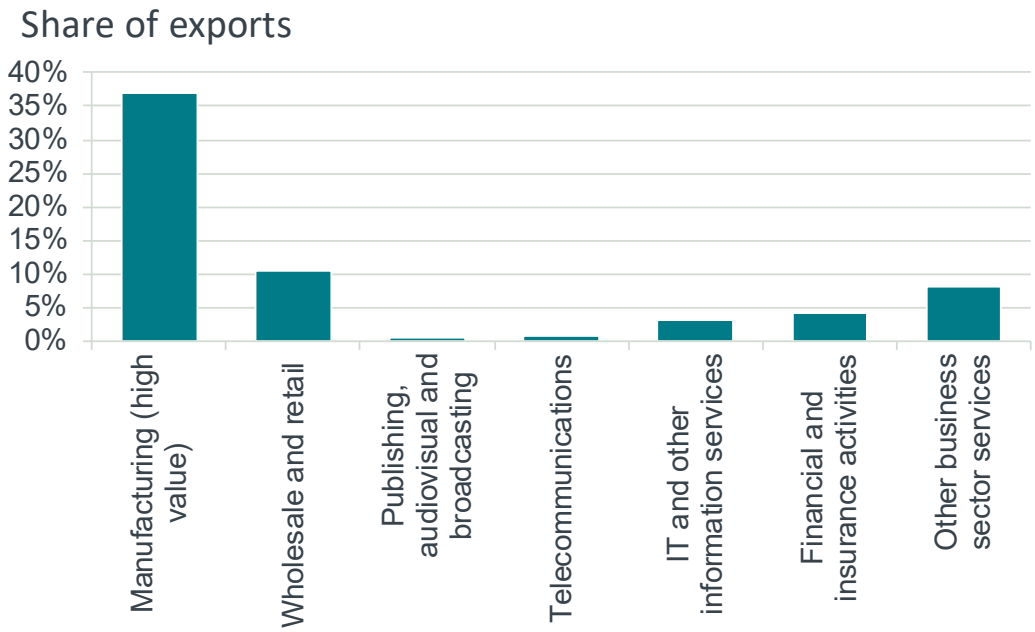
Figure 34 Share of EU's GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 35 reports the share of the different data-intensive sectors in EU exports. The figures can be usefully compared to the GVA figures. The comparison suggests that business services and wholesale/retail services have a strong domestic focus, whereas high value-added manufacturing has a stronger export orientation given its share of GVA.

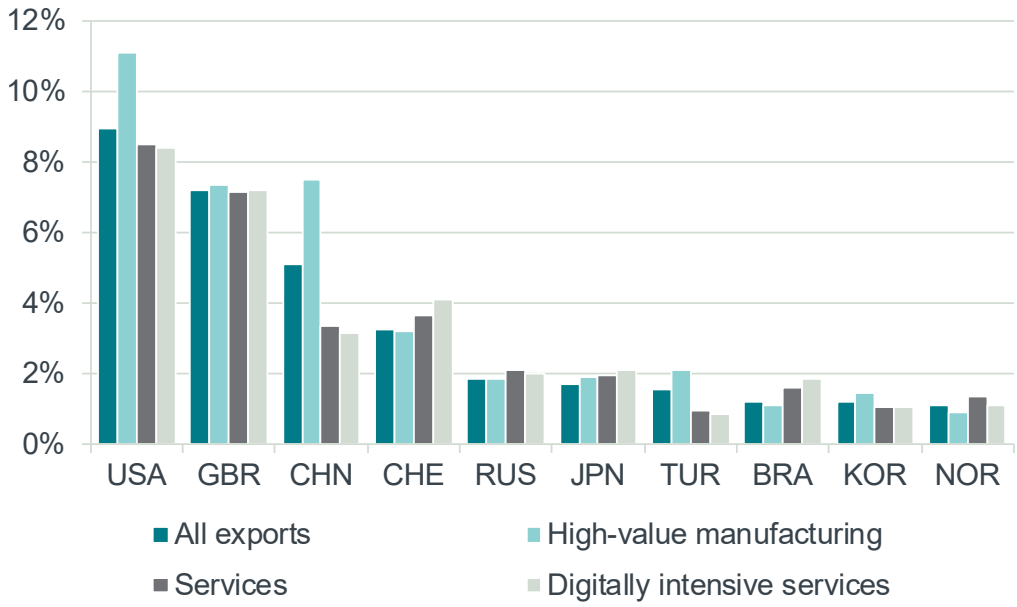
Figure 35 Digital/data-intensive sectors of exports share of exports



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 36 presents information on the EU's largest trade partners. Of the main partners listed, the EU has issued an adequacy determination for the UK, Switzerland and Japan. Norway falls under the scope of the GDPR by virtue of its membership of the EEA. A procedure for the adoption of an adequacy decision in respect of South Korea was launched in June 2021. The United States and the European Union negotiated arrangements under the aegis of the US-EU Privacy Shield, but these were invalidated as a consequence of a ruling by the ECJ in July 2020.

Figure 36 The EU's ten largest trading partners (percentage share by partner for export category)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset
Note: Data refer to 2015.

3.9.2 Data governance frameworks and localisation

Domestic legal and policy framework

The EU's framework for personal data governance is determined by the General Data Protection Regulation (GDPR), which came into force in 2018. Under Article 288 of the Treaty on the Functioning of the European Union (TFEU), all member states are required to comply with the provisions of the regulation. The regulation supersedes the domestic law of any member state on data governance.

The GDPR replaced the EU Data Protection Directive (95/46/EC), which was adopted in 1995. The EU Data Protection Directive, like all EU directives, had been implemented via domestic legislation of the member states. This had led to fragmentation in data protection regimes across the EU, which in turn had led to uneven levels of data protection and added business compliance costs.

Because the GDPR is a regulation, it is binding on member states without having to rely on domestic legislation, thus addressing to some extent the issue of fragmentation. This in turn is intended to facilitate the free flow of personal data within the EU and to support the development of the EU single digital market. At the same time, the GDPR identifies a number of areas in which member states have the permission to legislate differently via national laws, meaning that some degree of intra-EU variation will persist.

The territorial scope of GDPR is broad: it applies to the processing of personal data "in the context of the activities of an establishment" (Article 3(1)) of any organisation representative office, a subsidiary or agency), and those that supply goods and

services to EU residents and who, in the process of doing so, retrieve and store personal data. In effect, this means that the GDPR has an extra-territorial reach as it imposes obligations on non-EU businesses and institutions whose activities involve transactions with EU residents.

One of the core aspects of GDPR is its treatment of personal data in terms of the fundamental rights of data subjects. The GDPR recognises eight fundamental rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling.

The "rights-based" approach has implications for the way possible trade-offs between conditions imposed on personal data flows and the trade-facilitating effects of personal data flows are handled.

Non-personal data are handled by the Regulation of 2019 on the free flow of non-personal data within the single market. The European Commission in 2021 published proposal for a Data Governance Act. The purpose of the act is to stimulate the sharing of public and industrial data within the EU. The Act would also impose strict conditions that need to be met for data to transferred outside the EU. The approach to conditional cross-border extra-EU flows of data is similar to the approach underpinning GDPR. There are some concerns that this approach of using EU-data as a resource to stimulate an EU data-driven economy could entail data nationalism and costs associated with cross-border restrictions. [27]

Balancing trade benefits with other policy objectives

In regard to cross-border personal data flows with jurisdictions outside the EU, the EU's approach is to condition data flows on essential equivalence in data regulation. Specifically, it conditions data flows on the ability of partner countries to demonstrate that it offers protections on personal data that are deemed to be adequate in relation to those afforded by the GDPR. The European Commission makes a determination of adequacy based on an assessment of the partner country. The decision can be subject to review by the European Parliament and can also be challenged through the ECJ.

If adequacy has not been granted, data transfer can still take place through alternative contractual mechanisms such as standard contractual clauses

[27] Julie Balupo (2021)., T*he Data Governance Act: New rules for international transfers of non-personal data held by the public sector*, European Law Blog

authorised by the European Commission on the basis that these clauses provide adequate safeguards. Alternatively, transfers can take place under binding corporate rules (BCR). These are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. BCRs are subject to approval by the competent (usually national) data protection authority in the EU. While both standard contractual clauses and BCRs offer a route to data transfers where adequacy determinations are absent, they may present additional hurdles for smaller businesses.

The "fundamental rights approach" under GDPR nevertheless has significant implications for cross-border personal data flows. A demonstration of this is found in the ECJ rulings in successive cases ("Schrems I and Schrems II) that invalidated arrangements the European Commission had negotiated on behalf of member states with the United States to secure cross-border personal data flows. [28]

The findings of the ECJ have significant implications. They set a high bar for adequacy, making it a strong form of equivalence. Moreover, one of the implications is that the entire suite of instruments that enable cross-border personal data transfers (adequacy determinations, standard contractual clauses and BCRs) could be subject to judicial challenge and review at any time.

There is, at the time of writing, some uncertainty as to how the ECJ rulings will apply in practice. In November 2020, the European Protection Data Board issued its guidance regarding the implementation of the ECJ rulings. The guidance included a series of supplementary steps that businesses and organisations are required to undertake when transferring personal data to countries not benefiting from an adequacy decision. These steps include an assessment of the legal framework in the country in question and whether this enables compliance by the data importer with obligations under GDPR. If a determination is made that this is not the case, additional measures will be required by the data exporting business. The additional steps, in principle, induce additional compliance costs, which may affect smaller businesses disproportionately.

Relationship to trade agreements

Data provisions in the EU's FTAs are varied. Commitments in the EU-Japan FTA are limited to a rendez-vous clause committing parties to reassess the need for provisions on the free flow of data at a future date.

The EU-Canada CETA arrangement does not contain specific provisions mandating the free flow of data or banning data localisation. It states that efforts to ensure data protection should take account of international standards. The EU has granted an adequacy decision for commercial organisations in Canada.

[28] Respectively, Schrems v Data Protection Commissioner (2015) CJEU Case C-362/14 and Schrems and Facebook Ireland v Data Protection Commissioner (hereinafter "Schrems II")(2020) CJEU Case C-311/18.

The EU-Korea and EU-Singapore FTA agreements are more expansive in that they contain specific liberalisation commitments on data processing, data storage, data hosting or database services.

Finally, the EU-UK Trade and Cooperation Agreement (TCA) contains perhaps the most developed commitments on data in EU trade agreements to date. The TCA contains a chapter on Digital Trade. Article 201 commits both parties to ensuring cross-border data flows to facilitate trade and prohibits measures to restrict data flows. Prohibited measures include:

- Requiring the use of computing facilities or network elements in the party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a party;
- Requiring the localisation of data in the party's territory for storage or processing;
- Prohibiting the storage or processing in the territory of the other party; or
- Making the cross-border transfer of data contingent upon use of computing facilities or network elements in the parties' territory or upon localisation requirements in the parties' territory.

At the same time, Article 202 states that “each Party recognises that individuals have a right to the protection of personal data and privacy…”. Article Digit 202 further states that “Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred”.

These balancing provisions thus allow for parties to implement frameworks for the protection of personal data that stipulate conditions that need to be met in order for cross-border data flows to occur. In practice, an important determinant of the ease of cross-border personal data flows between the UK and the EU will be whether there are reciprocal adequacy arrangements between the EU and the UK.

Pursuant to the EU-UK joint declaration published alongside the TCA, there are currently reciprocal adequacy determinations (i.e. the UK’s determination of the EU and its member states and the EU’s determination for the UK), securing free cross-border flows of personal data between the parties.

The EU has also evolved a set of horizontal principles that provide a framework for the provisions it negotiates in trade agreements.

- Part A sets out prohibitions: on requiring the use of computing and network facilities in a territory as a condition of processing; on localisation of data for storage or processing; on storage and processing in the territory of another party; and making cross-border transfers conditional on localisation requirements or use of computing facilities.
- Part B sets out counterbalancing provisions by: stipulating that data privacy is a fundamental right; and presenting the safeguarding as a general exception, i.e. parties can maintain safeguards they deem appropriate.

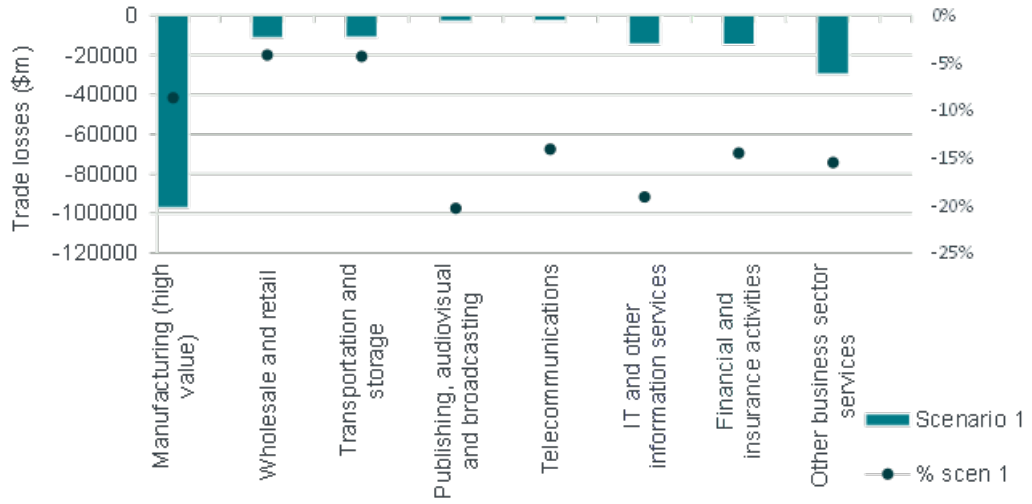
Part A goes beyond the requirements on data localisation in many current EU FTAs and if agreed with partners would support much deeper liberalisation commitments

than under the GATS or current practices. But Part B makes this conditional on parties adopting an approach to personal data protection similar to the EU's (based on fundamental right principles) creating a general exception across the agreement. Part B seems, on paper at least, to heavily qualify the liberalising potential of Part A. The evidence to date, based notably on the TCA, suggests that the European Commission has not sought to apply these principles (and notably Part B) *holus bolus* in the EU's trade agreements. However, their effects on future negotiations remains to be seen.

3.9.3 Modelling impacts of data localisation

We model the effects on the EU of a scenario in which it and its trade partners revert from current practice to full data localisation. This measures the value of trade at risk from a reversal of existing liberalisation or, equivalently, the value of safeguarding liberalisation achieved to date (for example, via standstill clauses in FTAs). The results are based on extra-EU trade and do not include trade between EU nations. Scenario 2 applied by the EU vis a vis the entire rest of the world would offset the impacts of scenario 1.

Figure 37 Impacts on the EU-27 of full data localisation



Source: Frontier Economics analysis based on OECD's STRI and TiVA datasets.

The EU starts from a relatively liberal baseline, so suffers relatively large impacts from restrictiveness in proportional terms. Services account for a third of EU exports, with sensitive sectors such as business services reasonably prominent.

The impacts are a combination of the EU's data localisation on its own exports, and of the impacts of trade partner localisation. The former dominate the latter: data localisation is bad for a country's export prospects. Read in light of the preceding analysis, the scenario could be conceived as one in which the EU rescinds commitments securing cross-border data flows vis a vis partners (whether in the form of an adequacy determination, a commitment in a FTA, or an equivalent arrangement) and the partners reciprocate in kind by rescinding commitments. To the extent that the EU's approach to data governance (including the jurisprudence around it) makes any arrangement or commitment potentially unstable, the results provide an upper bound to losses that might be associated with the instability of

GDPR in relation to guaranteeing the cross-border flows of personal data. The purpose of FTAs is usually to guarantee a certain threshold level of liberalisation that cannot be rolled back.

3.10 Conclusions

Most of the countries reviewed are liberal in the sense that restrictions on cross-border data flows are limited and the application of any restrictions are conditional on specified criteria. This ensures a level of predictability. India is an example of a jurisdiction where data localisation is on the rise. China has by far the most restrictive and most opaque requirements.

A shift to greater restrictions on cross-border data flows and away from current settings could generate significant negative impacts on all countries. Figure 38 reports the effects of the scenarios by country on trade and on GVA. GVA impacts are calculated using coefficients measuring the responsiveness of GVA to changes in trade (see section 4.2.3 and the technical annex for further information).

Figure 38 Summary of country-level trade and GVA impacts

Country	Trade impacts Scenario 1	Trade impacts Scenario 2	GVA impacts Scenario 1	GVA impacts Scenario 2
China	-3.6%	-2.7%	-0.9%	-0.7%
India	-7.1%	-5.9%	-1.8%	-1.5%
Japan	-7.3%	-6.4%	-1.8%	-1.6%
South Korea	-6.5%	-5.8%	-1.6%	-1.5%
Mexico	-8.1%	-7.9%	-2.0%	-2.0%
USA	-8.8%	-6.9%	-2.2%	-1.7%
France	-7.1%	-3.8%	-1.8%	-0.9%
EU	-6.7%	NA	-1.7%	NA

Source: Frontier Economics based on OECD data.

These impacts reflect a combination of the effects of the country's own data localisation measures and those of partners. A key finding is that a country's own data localisation measures have a bigger impact on its own exports than measures taken by partners (whether unilaterally or as retaliation): data localisation acts as a tax on a country's own exports. This is vividly brought out by the results for China, in which a unilateral reduction in data localisation from present high levels has a substantial positive effect on trade, which is nearly equivalent, in absolute value terms, to the combined effects of partners reverting to restrictive localisation policies.

The "export tax" effect of restrictions on cross-border data flows is in line with the effects of other forms of restrictions on services trade, and more of trade restricting measures on exports more generally. The reason this arises is that restrictions impose costs on businesses. These costs can take several forms. First, there are costs of compliance that can rise in line with propensities to operate internationally. Secondly, data localisation can reduce the contestability of markets for data-related services, by raising the height of barriers to entry into these markets. This in turn increases the costs for domestic businesses in data-intensive sectors that rely on data as inputs into production processes. Both the compliance and input

cost effects can be particularly relevant for businesses, particularly SMEs, that participate in global value chains. More broadly, and more subtly, costs stemming from restrictions (like other regulatory measures) raise the height of barriers to entry to domestic markets for the data-intensive industries themselves. This sheltering effect can make production by incumbents for the domestic market more attractive relative to overseas markets.[29] These effects are separate to longer term dynamic effects that reflect the impacts of restrictions on innovation, and that may further both the global competitiveness of businesses, and growth prospects, over time (see discussion below).

The modelling evaluated the impacts of data localisation by considering a shift from current settings towards restricted settings. Certain commonalities can be observed across countries:

- The highest absolute effects are observed in high-value manufacturing, reflecting the size of these sectors in trade and the importance of data to the operation of these sectors. The exception is India, where the effects of data localisation on IT services are greater.
- In proportionate terms, services sectors tend to be more heavily impacted. This reflects their high degree of data dependency, notably in publishing, IT and telecoms, financial and business services. For some countries, negative impacts are between a fifth and a quarter of exports. Absolute values are also high in certain cases, notably:
  - Financial services in the USA
  - Business services in the USA and the EU
  - IT and computer services in India.

It is possible that the reported GVA effects understate the costs of restrictions on cross-border data flows (and conversely the benefits of arrangements that secure cross-border data flows). In particular, data are important for nascent activities, such as Artificial Intelligence (AI). This is because access to large quantities of data are critical to the development of AI technologies such as neural networks and ensemble learning. These technologies also carry significant potential to boost productivity and thus long-term growth.[30] Restrictions on access to data increase the costs of developing the algorithms that underpin these technologies. While regulatory complexity, including uncertainty about the future direction of regulation, can also lead businesses to divert resources from innovation activities per se to compliance.[31]

These effects collectively mean that restrictions on cross-border data flows can have long run effects on the pace of development of new technologies, and in turn

[29] See for example, Bauer, M., Lee-Makiyama, H., van der Marel, E. and Verschelde, B. (2014), The Costs of Data Localisation: Friendly Fire on Economic Recovery, *ECIPE Occasional Paper no.3/2014*, ECIPE; and Australian Government (2015), *Barriers to Growth in Services Exports*, Productivity Commission Research Report, pp 150-151

[30] See notably Ajay Agrawal, Joshua Gans, and Avi Goldfarb (2019), The Economic of Artificial Intelligence; An Agenda, for a discussion of the potential effects on productivity of AI, and also the role of data flows in stimulating the development of AI.

[31] JE Bessen, SM Impink, L Reichensperger, R Seamans (2020) GDPR and the Importance of Data to AI Startups. NY Stern Business School; and Lee, Y S, B Larsen, M Webb, and M Cuéllar (2019), "How would AI regulation change firms' behavior? Evidence from thousands of managers", SIEPR Working Paper 19-031

affect their growth enhancing potential. The quantitative framework we have deployed is, at best, imperfectly suited to capturing the effects of nascent technologies that could, over time, have significant productivity-boosting impacts.

But even with these caveats in mind, the modelled effects underscore the value of data provisions in international trade agreements. They may further liberalisation, but even if they do not push liberalisation forward, they may set limits on how far countries can roll back existing levels of liberalisation. This would protect countries from the types of adverse impacts discussed above. These adverse impacts can be viewed as the costs that can be avoided through good quality FTA provisions that at least lock-in existing levels of liberalisation. As these adverse effects are generated by one's own data localisation measures, trade agreements act as a discipline on a country's own policy, and indeed provide a measure of security for sectors that depend on data flows in the face of pressures to restrict such flows.

Moreover, the raw results may understate some of the benefits of the locking-in effects of FTAs. This is because locking-in reduces uncertainty. In the presence of uncertainty, businesses may need to make inefficient investment decisions. For example, they may scale back activities in a country or postpone entry because they do not know how far these might be susceptible to changes in data localisation requirements. Or they may invest in data storage infrastructure as a precaution against future changes, which in turn is likely to increase the costs of doing businesses and prices charged to users and consumers.

For the non-European countries studied, the results suggest that while reciprocal arrangements with the EU can have significant trade-boosting effects, it is also very important for these countries to secure arrangements on a broader basis with other partners. Indeed, for the non-European countries covered in this report, the exposure of their trade to data localisation measures undertaken by non-EU countries is usually greater than it is to data localisation measures undertaken by the EU.

4 DATA LOCALISATION AND ITS IMPACTS ON THE UK

4.1 Background and context

The UK's data governance regime has, to date, reflected the implementation of the EU's GDPR via the UK General Data Protection Regulation. Following the UK's departure from the EU and the end of the transition period provided for under the UK-EU Withdrawal Agreement, the UK is no longer bound by the provisions of the EU-GDPR, but it has essentially been transposed into UK legislation via the UK DPA and the UK-GDPR.

Now the EU has determined that the UK's regime for data governance is adequate from the perspective of the EU-GDPR, there are reciprocal adequacy arrangements in place. At the same time, having left the EU, the UK has the opportunity develop its own data governance framework. According to the National Data Strategy (NDS), the UK will establish independent capability to conduct the UK's own data adequacy assessments. The NDS also states that the UK should have "a regulatory regime that is not overly burdensome for smaller businesses and that supports responsible innovation" and "maintain[s] a pro-growth data regime that the public trusts". Some commentators have interpreted this to indicate a relaxing of data protection standards relative to the European model.

The UK has also engaged in trade negotiations with external partners which include provisions relating to data and specifically cross-border data flows. It has notably concluded a FTA with Japan (see section 2.2.3) which includes provisions on data, and it has also applied to accede to the CPTPP.

In the remaining sections, we analyse the impact of data localisation policies on the UK. The approach followed is similar to that adopted for the countries analysed in section 3. We extend the analysis in several ways, by:

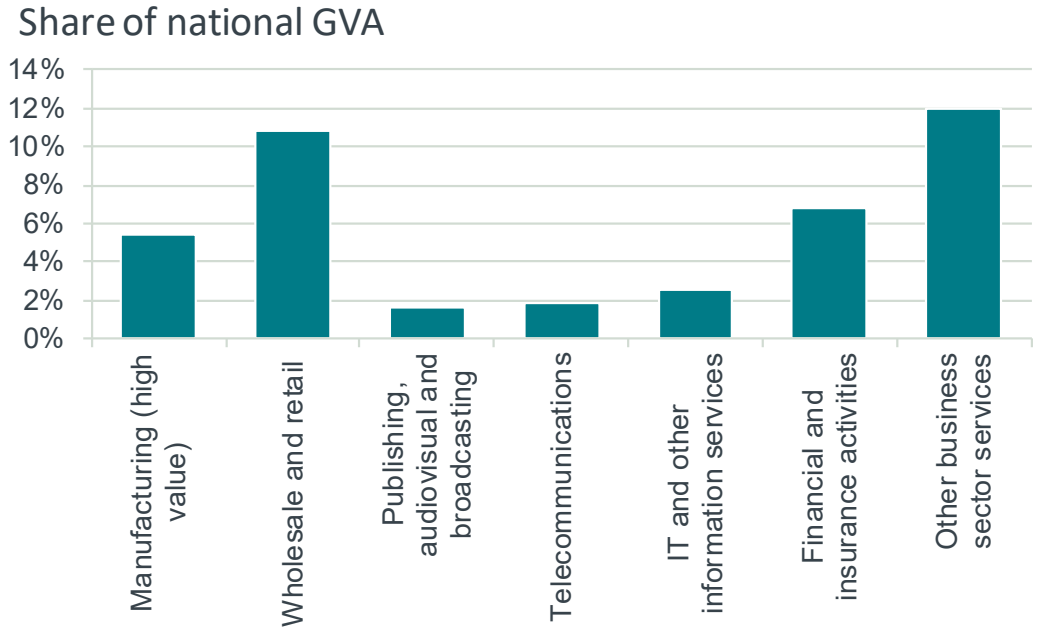
- Modelling an additional scenario, namely that the UK concludes an agreement with the USA and Mexico which mirrors the USMCA in its data provisions, and that it concludes data provisions along CPTPP lines with CPTPP countries and South Korea: and
- Measuring the regional impact of data localisation and disaggregating effects by firm size.

4.2 Modelling impacts

4.2.1 Background

Figure 39 underscores the particularly services-intensive nature of the UK economy. Though the relative shares of GVA accounted for by the sectors are somewhat similar to those seen in other countries, the share of high-value manufacturing in GVA is the smallest of all the countries considered and around half of that reported for the EU-27.

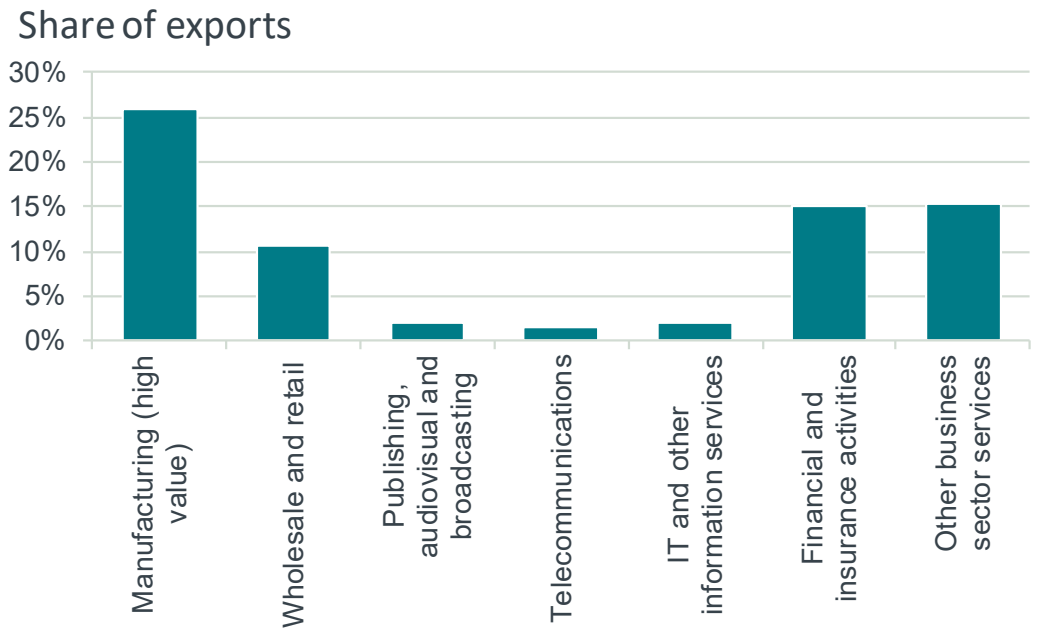
Figure 39 Share of UK GVA by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

The UK is particularly reliant on data-intensive exports. Over 70% come under this heading. As with most of the countries reviewed, high-value manufacturing is the leading sector, but three services sectors (financial and insurance activities, other business services, and wholesale and retail) collectively account for around 40% of exports. Within services, digitally intensive services represent two-thirds of exports, and only India, via the size of IT, has a higher share.

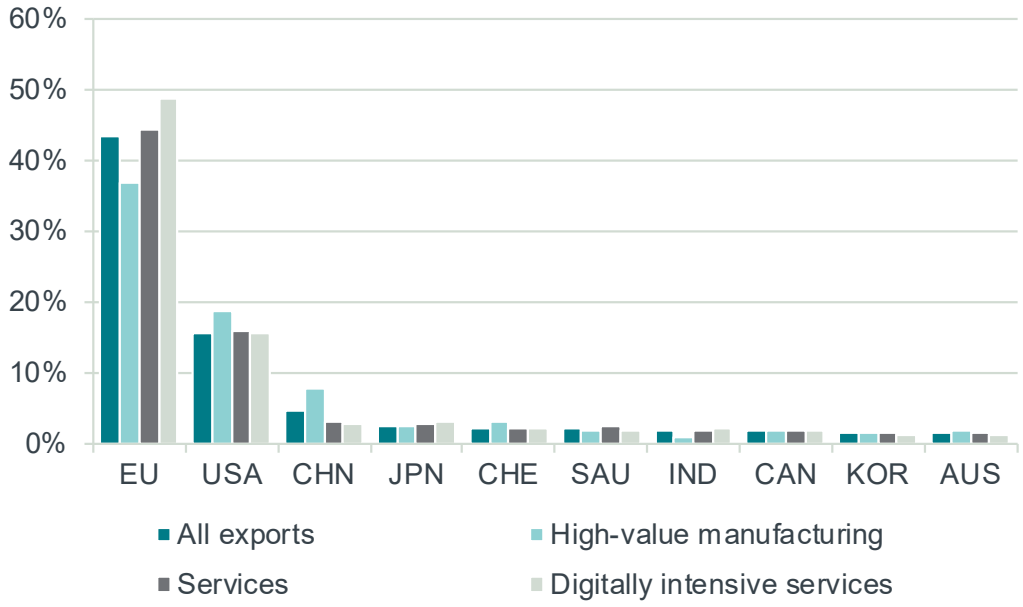
Figure 40 Share of UK exports by data-intensive sector



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

Figure 41 reports the direction of trade for the UK. We see that the EU is the largest trade partner and that this importance is particularly pronounced for digitally intensive services, where it is higher than the share for all exports and all services.

Figure 41 Top ten trading partners for the UK (percentage share of exports by country by major category of exports)



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.
Note: Data refer to 2015.

4.2.2 Scenario analysis

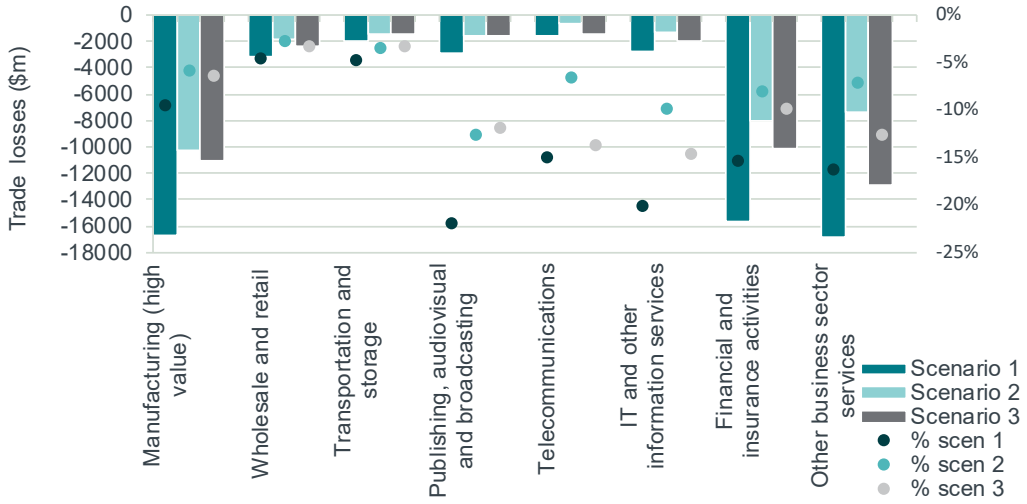
We model the following scenarios

- Scenario 1: We assume that the UK and its trading partners move from current practices to high levels of restrictiveness. This provides an estimate of the value at risk. As such a move would be (largely) GATS-consistent, this analysis indicates the value of locking in current levels of liberalisation, e.g. via a FTA.
- Scenario 2: Starting from full restrictiveness, we assume that the UK and the EU enter into reciprocal arrangements that liberalise cross-border data flows between them, in the same manner as was assumed to happen between the EU and the countries modelled in section 3. The difference between this scenario and the first scenario represents the incremental value to the UK and EU of reciprocal liberalisation of data flows when measured against a restrictive starting point
- Scenario 3: Starting from full restrictiveness under scenario 1, we assume that the UK concludes FTAs with the USA and Mexico along USMCA lines and concludes data provisions along CPTPP lines with CPTPP countries, and South Korea (which is in the process of acceding to CPTPP). The difference between this scenario and scenario 1 represents the incremental impact, for

the UK and partners, of entering into reciprocal agreements that liberalise cross-border trade.

. Figure 42 reports the results for each of these three scenarios

Figure 42 UK: impacts of data scenarios on trade



Source: Frontier Economics analysis of the OECD's Trade in Value Added (TiVA) dataset.

The UK starts from a liberalised starting point and trades predominantly with liberalised jurisdictions, so restrictions have a substantial impact. In contrast to most of the other countries studied in this report, the effects in absolute terms under scenario 1 for, respectively, financial and insurance services and other business services, rival or exceed the impacts on high-value manufacturing. The relative effects are much larger for these two services sectors than they are for high-value manufacturing and are broadly comparable to those reported for the other countries.

In scenario 2, the impacts in absolute terms on financial and insurance services and on other business sectors have nearly been halved and have also substantially fallen in high-value manufacturing. This reflects the importance to the UK of reciprocal arrangements with the EU regarding data.

Under scenario 3, impacts have also fallen relative to scenario 1, but not by as much for most sectors (wholesale and retail, transport and storage, and publishing are exceptions). The differences between scenarios 3 and 2 are also less pronounced with high-value manufacturing compared to other business services.

Both scenarios 2 and 3 point to the benefits to the UK and its partners of securing reciprocal arrangements that secure cross-border data flows. As observed in this report, the ways jurisdictions approach the question of cross-border data flows reflect broader regulatory architectures. Therefore the negotiation of reciprocal arrangements, and specifically the extent to which they can limit the scope for and impacts of data restrictions, will reflect the extent of differences in these architectures across partners.

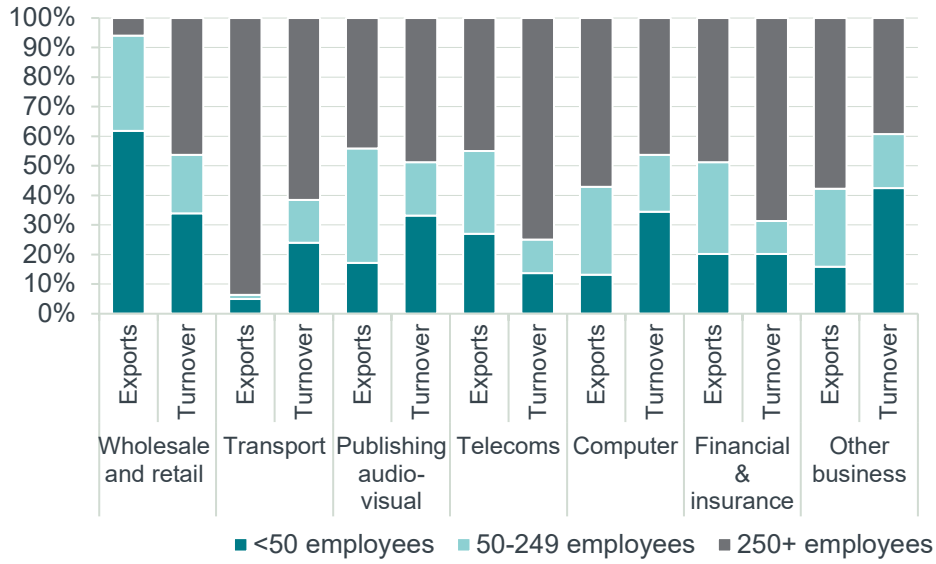
4.2.3 Regional and firm-level analysis

We explore how different parts of the UK economy are affected by analysing in detail how the trade impacts pan out in terms of regions and firms of different sizes. This is done by calculating region and size band shares of exports and apportioning out trade impacts on the basis of their export share. We can then compare with wider output at the region/size band level to look at the impacts in proportional terms. At the region level, we find that the services export base is heavily London-focussed. However, there is less of a pronounced pattern in terms of firm size.

Firm size effects

We apportion trade impacts to firm size using the ONS International Trade in Services (ITIS) microdata. For comparison, we also show how turnover is split between the size bands to give an indication of the relative export propensity of different firm sizes. For example, looking at Figure 43, we can see that, in terms of exports and turnover, large firms (250+ employees) typically account for around half of both exports and turnover. Comparing the export and turnover columns, in many cases they are fairly similar, which means that the propensity to export does not vary much with firm size. On closer inspection, the 50-249 employees band generally has a higher share in exports than in turnover, indicating a higher export propensity. This is consistent with the hypothesis that smaller firms are unlikely to export, whereas the high turnover in the 250+ band is driven by large firms serving the domestic market. Some sectors have notably different patterns: wholesale and retail exports are heavily weighted towards small firms, whereas turnover in the sector is not;[32] the opposite is the case for transport.

Figure 43 Attribution of exports and turnover to size bands



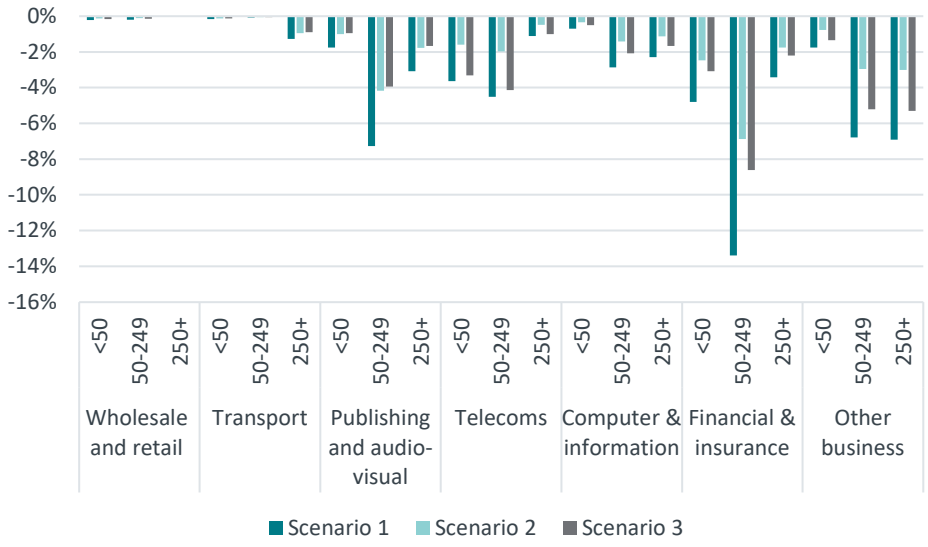
Source: *Frontier analysis of ONS ITIS, Business Population Estimates, and Annual Business Survey data.*

Note: *Data for manufacturing not available; construction data are disclosive; financial services turnover apportionment uses employee count.*

[32] Presumably, this reflects the turnover including large chain retailers, which are not relevant from an export point of view.

Trade impacts by sector and size band are derived by taking the sector-level export reductions from the scenario analysis and allocating these to the size bands in proportion to their export share. We then divide through by overall turnover to show the export impacts relative to their wider business, i.e. serving both domestic and export markets. In Figure 44 we show export reductions as a percentage of overall turnover, cut by size band and sector.[33] The differences in impacts across sectors reflect both their reliance on exports (as opposed to domestic markets) and the sensitivity of trade with respect to the STRI.[34] The differences by size band within a given sector reflect their different rates of export reliance.

Figure 44 Trade impacts as a proportion of firm turnover, by sector, size band and scenario



Source: *Frontier analysis of ONS ITIS, BPE and ABS data.*

Note: *Data for manufacturing not available; construction data are disclosive; financial services turnover apportionment uses employee count.*

Regional effects

We use two sources for regional apportionment. The first is the ONS ITIS experimental statistics, which capture the fact that London-headquartered firms may have activity elsewhere and so some exports should be attributed to those other locations. Broadly speaking, around half of digitally intensive services exports emanate from London. The second source, used for high-value manufacturing, is HMRC regional trade statistics. The data are rescaled into £ to reconcile with 2018 ITIS and HMRC totals, which allows for comparison with wider GVA at the regional level. The percentage trade impacts are shown in Figure 45 below.

[33] The same relativity of impacts between size bands would be seen in the other scenarios, Note that we do not model differences in destination mix between size bands within a sector.

[34] For example, although computer and financial services both show similar export reductions in percentage terms (see Figure 42) as a proportion of turnover, the impacts are much larger for financial services, which are a result of it being a more export-reliant sector.

Figure 45 Trade impacts by region (%)

Region	Scenario 1	Scenario 2	Scenario 3
North East	-7.7%	-3.5%	-5.6%
North West	-7.9%	-4.9%	-5.2%
Yorkshire and The Humber	-6.5%	-3.3%	-4.5%
East Midlands	-8.4%	-4.8%	-5.7%
West Midlands	-8.1%	-5.1%	-5.2%
East of England	-7.8%	-4.7%	-5.2%
London	-10.7%	-5.2%	-7.6%
South East	-8.9%	-4.7%	-6.3%
South West	-8.0%	-4.6%	-5.3%
Wales	-6.1%	-2.7%	-4.5%
Scotland	-6.1%	-3.6%	-4.0%
Northern Ireland	-8.2%	-4.5%	-5.7%
UK total	-8.6%	-4.6%	-5.9%

Source: Frontier analysis of TiVA, STRI, ITIS, and ABS data.

The difference in impacts between regions is driven by their sector mix: London is most heavily impacted in this case because its exports are more heavily weighted towards export sectors that are more affected by data restrictions. By contrast, regions dominated by exports of agriculture and primary products will be less affected.

We also account for whether the export destination is EU or non-EU. Comparing scenarios 1 and 2, if a region trades more heavily with the EU, then the dampening effect of reciprocal arrangements with the EU will be greater. For example, with London, the scenario 2 impacts are less than half as large as in scenario 1, whereas the impact reduction for the West Midlands is less pronounced.

Gross value added impacts

We can then translate the impacts into gross value added (GVA) terms, which allows us to see how much value overall to the economy is lost as a result of impeded trade. This also allows us to understand the magnitude of the impact relative to the size of the regional economy. We begin with a “bottom-up” approach which focuses on the direct impact on the exporting sectors, and which can be moderated by impacted jobs moving to less productive activities. This can be considered a lower bound, as there may be wider impacts on inputs into the importing sector.

The first stage in the bottom-up/direct approach is to convert the trade impacts which are on a turnover basis into a GVA basis. In the case of services, around half of output is value added with the other half representing inputs. For manufacturing, inputs take a higher share. As a conservative assumption, we focus only on the direct value-added component without stipulating what happens to the inputs.

We then divide through by GVA per employee to derive the number of impacted employees.[35] In other words, this is saying: if these exports were lost how many jobs would that account for? This is shown in Figure 46.

Figure 46 Number of impacted employees by scenario

Region	Scenario 1	Scenario 2	Scenario 3
North East	-6,050	-2,781	-4,441
North West	-16,344	-9,476	-11,095
Yorkshire and The Humber	-9,344	-4,681	-6,601
East Midlands	-11,063	-6,263	-7,583
West Midlands	-16,235	-9,948	-10,724
East of England	-18,618	-11,628	-12,270
London	-122,153	-54,996	-90,464
South East	-45,005	-23,612	-32,217
South West	-11,349	-6,393	-7,730
Wales	-5,583	-2,553	-4,108
Scotland	-18,537	-10,226	-12,745
Northern Ireland	-3,314	-1,620	-2,426
UK total	-283,593	-144,175	-202,404

Source: Frontier analysis of TiVA, STRI, ITIS, and ABS data.

Consistent with Green Book principles, to calculate net GVA impacts, we assume that rather than outright job losses, workers instead move into less productive jobs. The net GVA impact therefore is given by multiplying the number of impacted jobs by the difference between GVA per employee in the impacted sector and GVA per employee in the wider economy.[36] In practice, there will be constraints on the speed and extent to which these reallocation effects play out. We abstract from these, meaning that the results are likely to be conservative in the sense of understating the extent of losses.

The next GVA impacts are shown in Figure 47. To summarise scenario 1: there are net losses of GVA in the region of £10 billion relative to overall GVA of £1.9 trillion, giving a 0.6% reduction overall. Of the regions, London is most heavily impacted. This is because it is more open to trade than other regions and is focussed on export sectors that are more sensitive to data restrictions.

[35] The conversion of turnover to GVA and jobs uses Annual Business Survey data.

[36] So if exports in sector A are £100m and GVA represents 50% of turnover, then £50m of GVA is directly impacted. If GVA per employee in sector A is £100k per head, the £50m GVA loss means there are 500 jobs lost in sector A. Suppose the wider economy has GVA of £50k per head, and the impacted employees find employment in the wider economy, then the net impact on GVA would be 500 impacted jobs x (£100k p/h in sector A - £50k p/h in wider economy) = £25m.

Figure 47 Net GVA impacts using bottom-up approach

	£m				%		
Region	Total	Scen 1	Scen 2	Scen 3	Scen 1	Scen 2	Scen 3
North East	54,631	-305	-144	-217	-0.6%	-0.3%	-0.4%
North West	183,162	-698	-396	-458	-0.4%	-0.2%	-0.3%
Yorkshire and The Humber	123,612	-455	-232	-307	-0.4%	-0.2%	-0.2%
East Midlands	108,966	-476	-274	-316	-0.4%	-0.3%	-0.3%
West Midlands	141,405	-801	-496	-518	-0.6%	-0.4%	-0.4%
East of England	164,580	-649	-385	-423	-0.4%	-0.2%	-0.3%
London	450,278	-3,967	-2,028	-2,694	-0.9%	-0.5%	-0.6%
South East	277,256	-1,403	-704	-996	-0.5%	-0.3%	-0.4%
South West	139,381	-559	-317	-369	-0.4%	-0.2%	-0.3%
Wales	65,089	-299	-135	-217	-0.5%	-0.2%	-0.3%
Scotland	142,121	-691	-401	-443	-0.5%	-0.3%	-0.3%
Northern Ireland	42,201	-146	-80	-102	-0.3%	-0.2%	-0.2%
UK	1,892,682	-10,449	-5,593	-7,059	-0.6%	-0.3%	-0.4%

Source: Frontier analysis of TiVA, STRI, ITIS, and ABS data.

The step of using only direct GVA (i.e. focusing on the direct GVA component and losing the rest of the turnover accounted for by inputs) could be argued to be overly conservative on the basis that the intermediate inputs would also be impacted. But it can be considered consistent with the full employment model, under the assumption that the inputs have GVA per employee in line with the wider economy. That is, we assume that even if input providers are impacted, they would continue to carry out other economic activity with the same productivity.

We complement the approach above with a "top-down" approach that draws on wider relationships between trade and GVA, which allow for mechanisms such as knowledge spillovers between businesses and industries that boost productivity. For example, as firms compete in world markets, their efficiency increases through learning-by-doing effects. These can flow to other firms through the movement of employees or through observation.

We also explore an alternative approach to GVA impact using top-down estimates of the relationship between trade and productivity at the macro level. Here we draw on HM Treasury research[37] which focuses on a trade openness-productivity elasticity range of 0.2 to 0.3. Using a mid-point of 0.25 means that a 1% increase in trade would be associated with a 0.25% increase in GVA in the long run. This approach suggests that the GVA reductions associated with scenarios 1-3 would be 2.2%, 1.2% and 1.6% respectively. This is around four times as large as the bottom-up estimates. It could be argued that the latter approach is overly conservative as it does not model any changes to intermediate inputs, the full employment assumption may not be appropriate and there are various mechanisms through which wider spillover effects may occur. For this reason, we would consider the top-down and bottom-up approaches to give upper and lower bounds on the range of potential GVA impacts. At the same time, it is possible that,

[37] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517154/treasury_analysis_economic_impact_of_eu_membership_print.pdf para A.127

for the reasons given in section 3.10, that the top-down approach does not capture some of the growth effects of cross-border data restrictions via their effects on the development of productivity-enhancing new technologies.

5 QUALITATIVE ANALYSIS

5.1 Introduction

The purpose of the qualitative analysis is to provide a view from the firm-level perspective on data localisation. We seek to establish how far the concept is understood by businesses and how the concept translates into business operations, and with what impacts.

The qualitative analysis consists of two parts. The first is based on the findings of a YouGov omnibus panel. The second is based on in-depth interviews with a range of businesses.

5.2 Business survey

5.2.1 Background

To understand the level of awareness and impact of data localisation measures among British businesses, we commissioned a YouGov survey of businesses with a commercial interest in the UK which export to one of more countries of interest. Specifically, the sample of businesses includes those which export goods and/or services to China, USA, France, Germany, India, Russia, South Africa, Vietnam, Malaysia, South Korea, Japan, Poland, Australia, New Zealand and/or Mexico.

To ensure a sufficient-sized representative sample, we used a dedicated business panel of 2,000 respondents for this survey, of which 716 (36%) export to one or more of the listed countries for this study. This sample size allowed us to conduct subgroup analysis across different segments, including by country of export, sector and business size. Further, all results were weighted by business size and sector using underlying business data from Nomis, as provided by DCMS.[38]

To further develop our understanding of the awareness and impacts of data localisation measures and demonstrate the experience of businesses, we conducted a series of interviews with large businesses affected by such measures which operate across multiple countries. These interviews helped to contextualise and bring to life key findings from the survey by exploring how data localisation has affected these businesses and how they have and continue to address any challenges, e.g. impact of compliance costs such as diversion of activity to other jurisdictions.

The following sections set out our key insights and findings from this review, covering:

- An overview of key subgroups;
- How businesses store data;

[38] Nomis is a service provided by the Office for National Statistics, ONS, to give you free access to the most detailed and up-to-date UK labour market statistics from official sources

- Awareness of country-specific data localisation requirements and potential impact of any changes; and

5.2.2 Summary of key findings

As set out in the previous section, a key element of this review is the business survey covering 2,000 businesses with a commercial interest in the UK. Over 40% of businesses are focussed in the following sectors: retail (14%), construction (14%), hospitality and leisure (9%), and IT and telecoms (8%). The key insights and findings based on the analysis of these results are summarised below:

- Among businesses which export to one or more of the listed countries, **the key countries of export are the USA, France and Germany** (with over 60% of businesses in the sample exporting to at least one of these countries). This is broadly consistent across different types and sizes of businesses.
- There was **limited agreement** among senior decision makers (SDMs) **on the importance of their businesses investing in data storage** in the countries of their customers as an important part of business strategy. Eighteen percent of businesses which hold personal data agreed that their business invests in data storage in the countries of their customers because this is an important part of their business strategy, while over 40% disagreed.[39]
- There was **relatively limited awareness** among SDMs regarding **requirements around storing or transmitting data** to countries. Over a third of businesses which import or export goods or services in the listed countries and hold personal data stated they were not aware of the nature of the country-specific requirements or whether indeed there were any specific localisation requirements. Awareness did not increase with firm size. There may be some sectoral effects with finance, professional services, transportation, legal and IT/telecoms showing higher levels of awareness.
- Further, **under a third of businesses which export to each of the listed countries agreed that these countries have a "clear governance framework"** on how cross-border data flows are handled, reflecting an overall limited understanding of such governance frameworks across all the listed countries of export. This varies across countries of export:
  - 22% to 32% of SDMs who export to **France, Germany and Poland** agreed that these countries have **a "clear governance framework"** on how cross-border data flows are handled, the highest of all the listed countries. Cross-border flows of personal data in France, Germany and Poland (in line with the rest of the EU) are governed by GDPR. The relatively high results for these countries may partly indicate *relatively* greater clarity on the regulation around cross-border personal data flows for these countries compared to the others, reflecting the substantial effort put in by the European Commission and other government bodies in disseminating information on the GDPR and not least because of the extra-territorial reach of the GDPR relative to some other country data governance frameworks.

[39] The remainder of the group fall in the "don't know" or "neither agree nor disagree" categories.

- Across the rest, businesses which export to countries with relatively less restrictive data regimes tend to have a higher degree of agreement on the clarity of these regimes (e.g. USA and Australia at 18% each) relative to businesses which export to countries with more restrictive (and arguably opaque) data regimes in place (e.g. India, China and Russia, where this stands at less than 5%).

- **Over 50% of businesses which export goods and/or services** to the listed countries believed they would be **negatively impacted** if countries that their business operate in required that all personal data from clients and employees in those countries had to be stored exclusively in those countries.
- **GDPR is broadly recognised as the key regulation on data protection**; over 56% of businesses recognise GDPR as the highest standard of data protection. Further, close to 70% of businesses stated that they apply GDPR guidelines as a standard across all countries they operate in, even where GDPR is not a requirement in these countries.

5.2.3 Detailed insights and findings

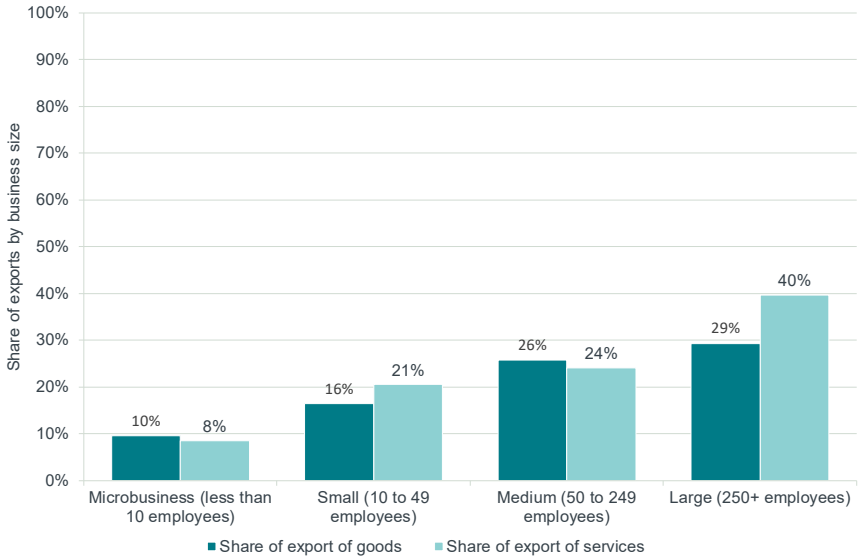
This section sets out in more detail the key insights and themes summarised above, based on our analysis of the survey results.

Overview of key subgroups

The sample of businesses covers businesses across different sizes and sectors. Over 99% of businesses are SMEs (1 to 249 employees), of which over 90% are microbusinesses (fewer than 10 employees). Large businesses (250+ employees) are less than 1% of the overall base.

As shown in Figure 48, the share of businesses exporting goods or services tends to be higher for larger businesses than smaller ones, with the export of services being more prominent compared to the export of goods for large businesses. For instance, 10% of microbusinesses export goods and 8% of them export services, compared to 29% and 40% respectively for large businesses.

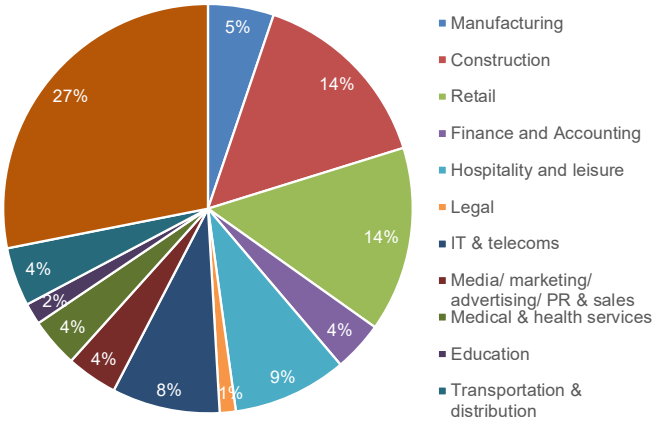
Figure 48 Share businesses export by business size



Source: YouGov business survey; Frontier analysis.

Over 40% of businesses are focussed in the following sectors: retail (14%), construction (14%), hospitality and leisure (9%), and IT and telecoms (8%). Construction, at 27%, is the single largest sector. This is illustrated in Figure 49.

Figure 49 Distribution of businesses by sector



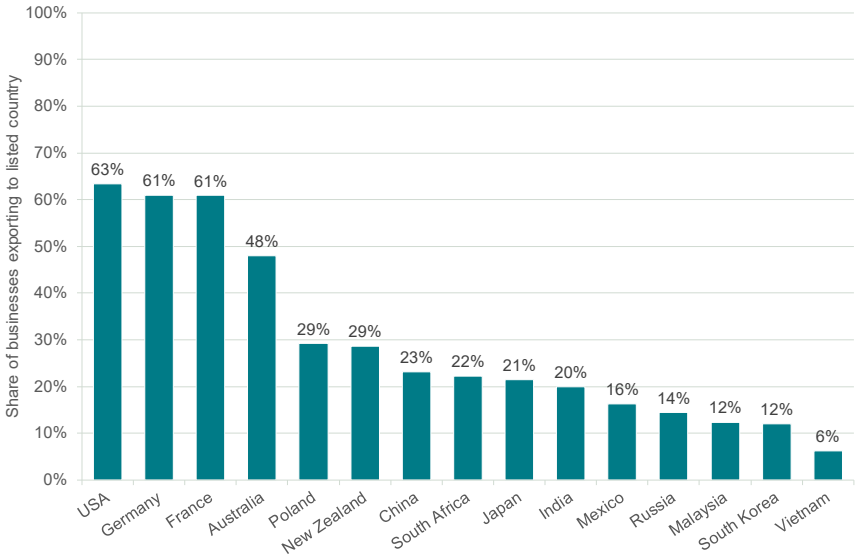
Source: YouGov business survey; Frontier analysis.

Among businesses which export goods and/or services to one or more of the listed countries, the key countries of export in our sample of businesses are the USA, France and Germany (with over 60% of businesses in the sample exporting to at least one of these countries). This is broadly consistent across business sizes. The share of exports by country is illustrated in Figure 50.

This is also consistent with country-level data which show that the EU is the UK's largest trading partner (accounting for 37% of high-value manufacturing and nearly half of digital-intensive services exports), followed by the USA.[40]

[40] OECD Trade in Value Added (TiVA) dataset.

Figure 50 Distribution of businesses by country of export



Source: YouGov business survey; Frontier analysis.

Data storage and importance

Businesses largely store data through cloud storage providers or internal company storage systems (17% and 31% respectively), with only 7% using other third-party storage systems. Across business sizes, a greater proportion of larger businesses tend towards internal storage systems compared to smaller ones, which tend to opt for cloud storage systems more often.

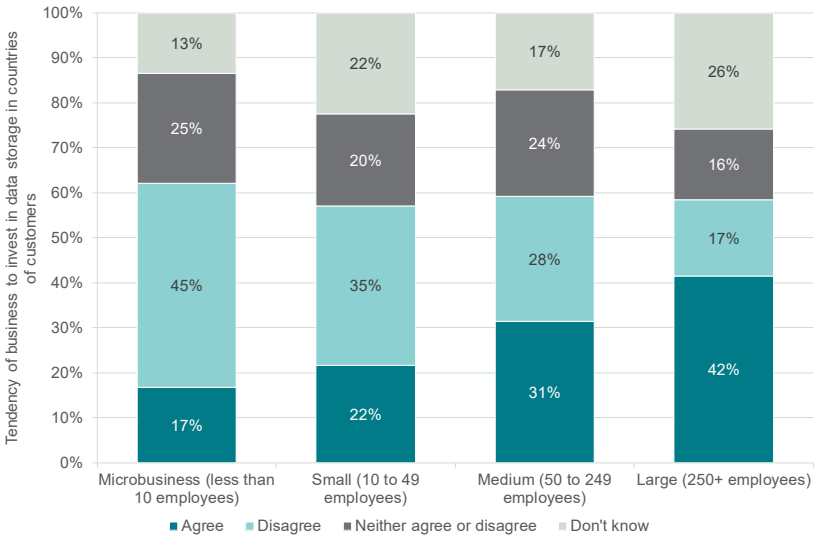
Overall, there was limited agreement among SDMs of businesses which hold personal data (in any of the forms mentioned above) on the importance of their businesses investing in data storage in the countries of their customers as an important part of business strategy. Eighteen percent of businesses which hold personal data agreed that their business invests in data storage in the countries of their customers because this is an important part of their business strategy, while over 40% disagreed. This is fairly consistent across countries of export although it varies by sector and business size.[41]

As shown in Figure 51, the tendency to invest in data storage in countries of their customers tends to be higher for larger businesses than smaller ones. Overall, 42% of large businesses which hold personal data agreed that their business invests in data storage in the countries of their customers because this is an important part of their business strategy (because it signals trust to consumers and because it mitigates exposure to litigation), relative to 18% for SMEs. This may in part reflect the relatively larger role of exporting as a part of the overall business model for larger businesses.[42]

[41] The remainder of the sample group fall in the "don't know" or "neither agree nor disagree" categories.

[42] OECD; "SMEs and International Trade", 2015. (https://www.oecd-ilibrary.org/docserver/entrepreneur_aag-2015-21-en.pdf?expires=1613642485&id=id&accname=guest&checksum=83338928376128668D4AA68AE5662887)

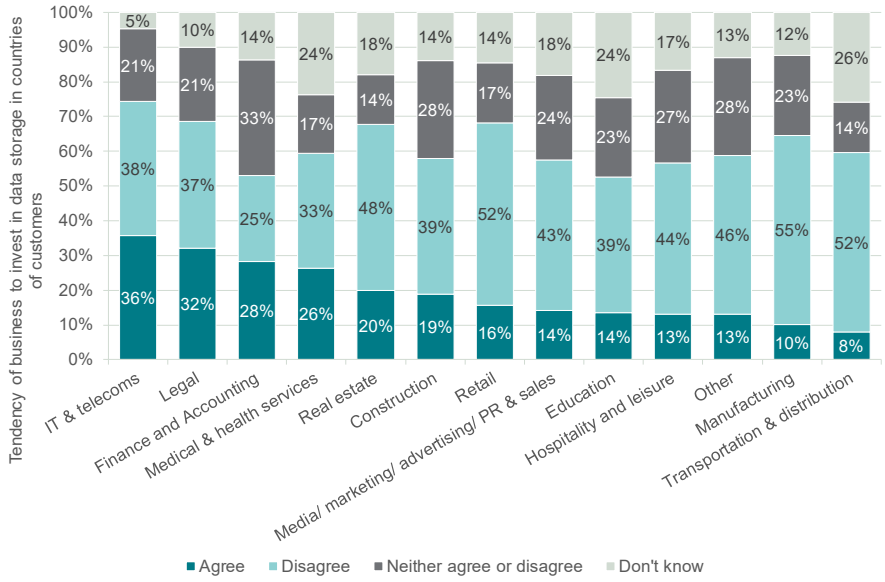
Figure 51 Response to statement "My business invests in data storage in the countries of our customers because this is an important part of our business strategy", by business size



Source: YouGov business survey; Frontier analysis.

Looking towards sectors, the share of businesses which agreed that they invest in data storage in countries of customers as an important part of their strategy is relatively higher for finance and accounting (28%), legal (32%) and the IT and telecoms sectors (36%) compared to the rest. This is illustrated in Figure 52 below.

Figure 52 Response to statement "My business invests in data storage in the countries of our customers because this is an important part of our business strategy", by sector



Source: YouGov business survey; Frontier analysis.

Awareness of country-specific requirements and potential impact of changes

A key objective of the survey was to understand businesses' awareness of data localisation measures in countries they operate in. Overall, the survey results indicate there is relatively limited awareness among SDMs of requirements around storing or transmitting data to countries, with over a third of businesses which import or export goods or services in the listed countries and hold personal data stating they were not aware of the nature of the country-specific requirements. Specifically:

- 40% did not know if there were requirements to store personal data in countries of export.
- 39% did not know if their business needed to comply with requirements before data were transmitted to countries of export.

Firm size does not seem to make a difference: levels of unawareness for SMEs versus large businesses (i.e. 250 employees or more) show roughly similar levels of unawareness. This is also fairly mixed across listed countries of export.

There is some evidence that certain sectors may be more aware: finance, professional services, legal, IT and telecoms, and transport have a relatively low proportion of respondents saying they were unaware whether their business needed to comply with requirements. However, the proportions (between around 20% and 30%) of those unaware is still relatively high.

Among the businesses which export to one or more of the listed countries, there also appears to be fairly limited understanding around the clarity of governance frameworks on how cross-border data flows are handled in these countries. Specifically, 51% stated they were not aware of whether countries of export have clear data governance frameworks that identify how cross-border data flows may be handled.

Further, under a third of businesses which export to each of the listed countries agreed that these countries have a "clear governance framework" on how cross-border data flows are handled, reflecting an overall limited understanding of such governance frameworks across all the listed countries of export.

While there is no clear pattern across business sizes, this figure varies considerably across countries of export: 22% to 32% of SDMs who export to France, Germany and Poland agreed that these countries have a "clear governance framework" on how cross-border personal data flows are handled. This is the highest of all the countries of export, followed by the USA and Australia at 18% each.

Cross-border flows of personal data in France, Germany and Poland (in line with the rest of the EU) are governed by GDPR. The relatively high results for these countries may partly indicate *relatively* greater clarity on the regulation around cross-border personal data flows for these countries compared to the others, reflecting the substantial effort put in by the European Commission and other government bodies in disseminating information on the GDPR, and not least because of the extra-territorial reach of the GDPR relative to some other country data governance frameworks.

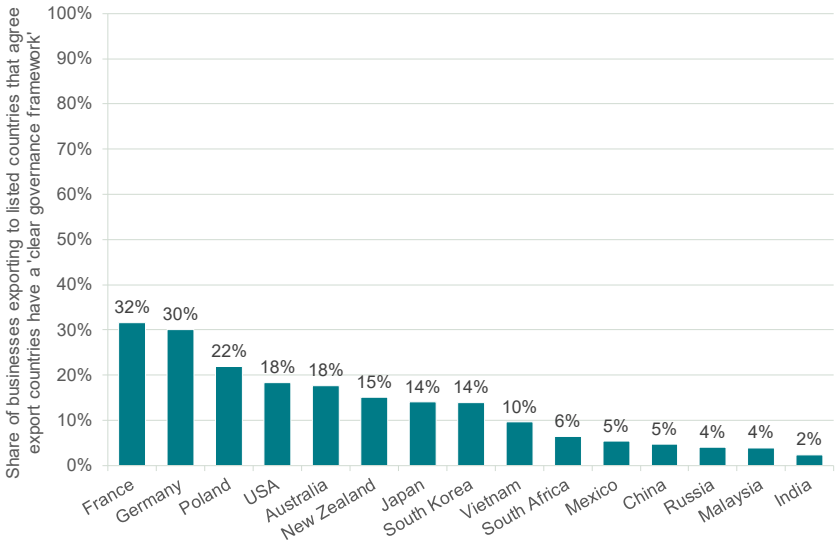
Across the rest, businesses which export to countries with relatively less restrictive data regimes tend to have a higher share of agreement on the clarity of these regimes relative to countries with more restrictive regimes in place.

The USA, in particular, is noted for having a relatively low level of restrictiveness around cross-border data flows, broadly operating on an "accountability" principle[43] with few limits on the transfer of personal data outside the USA. In Australia, data transferors are obliged to take "reasonable steps" to ensure data is protected abroad or have "reasonable grounds" that data will be protected abroad. This relatively less restrictive approach may contribute to the governance framework being easier to understand relative to some others, where the share of businesses agreeing the governance framework around cross-border data flows is clear is well under 10%.

In contrast, China, India and Russia are examples of countries with more restrictive (and arguably opaque) regimes around data protection. This may be a factor in the relatively low share of businesses which export to these countries agreeing that there is a "clear governance framework" on how cross-border flows are handled (2% to 5%).

The results for Mexico are interesting to note as well. Only 5% of businesses which export to Mexico agreed that there is a "clear governance framework" on how cross-border data flows are handled. This finding is notable as the FTA that Mexico has entered into with the USA includes fairly prescriptive obligations on cross-border data flows. In principle, this should have improved the transparency of Mexico's data regime but this is not yet evident (at least for British exporters).

Figure 53 Share of businesses that agree countries of export have a "clear governance framework" on handling cross-border flows



Source: YouGov business survey; Frontier analysis.

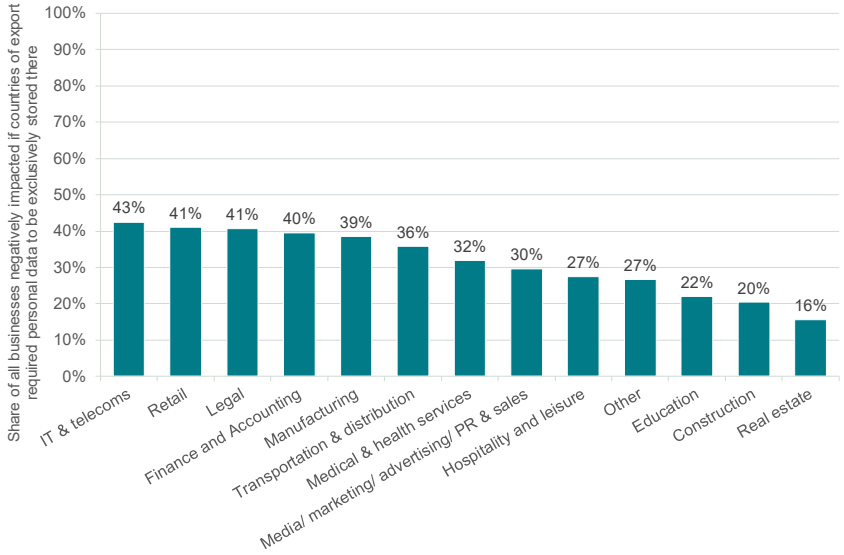
[43] Specifically, entities which export data remain liable in case of misuse.

While, overall, there appears to be fairly limited awareness of current country-specific data localisation requirements, over 50% of businesses which export goods and/or services to the listed countries believe they would be negatively impacted[44] if countries that their business operates in required that all personal data from clients and employees in those countries had to be stored exclusively in those countries. This is broadly consistent across the listed countries of export.

Across all the businesses in the sample, a greater share of larger businesses believe they would be negatively impacted compared to smaller ones. Fifty-four percent of large businesses[45] stated they would be negatively impacted by such a change in regulation vs. 31% of SMEs.[46]

This also varies to some extent across sectors. As shown in Figure 54, across all the businesses in the sample, the share of businesses that believe they would be negatively impacted is the highest (above 40%) among businesses focussed on the IT and telecoms, retail, legal, and finance and accounting sectors. At the other end, this stands at 16% to 22% for education, construction and real estate.

Figure 54 Negative impact of change in requirements to store personal data exclusively in countries of operation



Source: YouGov business survey; Frontier analysis.

5.2.4 Conclusions

The results of the YouGov business survey provide valuable insights on the level of awareness and impact of data localisation measures among British businesses.

The results highlight the importance of data localisation issues for businesses, with the majority of the businesses which export goods and/or services to the listed

[44] This includes all those which stated they would expect "large negative effects" or "noticeable negative effects" and excludes those which stated "negligible", "no" effects or "don't know".

[45] 250+ employees.

[46] 1 to 249 employees.

countries stating they would be negatively impacted if the countries that they operate in required that all personal data from clients and employees in those countries had to be stored exclusively in those countries.

Further, the survey found that businesses' awareness of country-specific requirements around storing or transmitting data to countries is relatively limited, with over a third of businesses which import or export goods or services in the listed countries and hold personal data stating they were not aware of the nature of the country-specific requirements or indeed whether these requirements exist. This could leave businesses vulnerable to sudden changes in policy or government action around data localisation requirements in specific countries. Such changes in legislation around cross-border data flows in countries of export could leave businesses exposed, resulting in a significant negative impact for these businesses. This echoes the findings of the quantitative results presented in this report.

This highlights the value of transparency in data localisation measures across key countries of export for British businesses (and more broadly) and the importance of businesses ensuring they have a solid understanding of the data requirements in place in countries that they are operating in. Overall, to enable this, this may suggest there is value in seeking data provisions in trade agreements to provide more predictability and transparency.

Going forward, it may be helpful to undertake further research to understand the nature and magnitude of any negative impact businesses may expect to deal with if faced with more restrictive data localisation requirements in countries of export and any measures businesses may already have in place to mitigate this.

Further, it could be helpful to explore what factors may be driving the limited awareness and clarity around country-specific data localisation regimes and what measures might be most effective in addressing this. For instance, outside of the EU countries, it appears that businesses which export to those with less restrictive data regimes have relatively higher awareness and understanding of data localisation requirements for these countries relative to those exporting to countries with more restrictive (and potentially opaque) regimes.

This could reflect a lack of awareness, partly because gaining familiarity with such regulations in countries that lack transparency requires a significant investment in resources. It might also reflect an assumption that enforcement in these countries is weak. The former point underscores the importance of transparency and information provisions in international agreements.

5.3 In-depth business interviews

5.3.1 Overview of approach and respondent group

A total of 12 in-depth interviews were conducted with representatives from UK businesses (including those with headquarters overseas) which export either goods and/or services.

Figure 55 Sectoral mix of interviewees

Sector of business	Number interviewed
Technology	3
Consultancy and professional services	2
Legal	1
Finance	2
Telecoms	2
Insurance	2

Figure 56 Interviewees by business size

Size of business (number of employees)	Number interviewed
Very large (more than 1,000 employees)	8
Large (250-999 employees)	1
Medium (50-249 employees)	1
Small (10-49 employees)	1
Micro (1-9 employees)	1

Interviewees were identified using a combination of DCMS business lists, the Dun and Bradstreet database and Frontier Economics contacts. It should be noted that, due to the implications of Covid-19 restrictions, this sample was highly self-selecting and not representative of the wider business population (who may be less engaged with this agenda or had limited capacity to respond to this at the time of conducting the interviews). The sample comprises representatives from organisations where data localisation is a key concern or known to be a consideration for their company, and/or where an appropriate respondent could be identified outside of furlough and work-from-home requirements.

Individual respondents varied in their roles depending on the size and nature of their business. They included those in governmental liaison roles, data protection officers and company CEOs.

5.3.2 Awareness of country-specific requirements

In-depth interviews found that respondents from both large and small companies are aware of data localisation requirements in the countries in which they operate (which contrasts with the generally low levels of awareness detected via the YouGov survey, likely due to the more engaged nature of the qualitative sample).

This is typically because the ability to store, transfer and/or process personal data is itself a key business activity, or because it plays a critical function facilitating business operations. Respondents reported having to be mindful of regulations in a range of territories including the USA, EU member states, Russia, Turkey, India, Israel, Australia, New Zealand, China, Japan, Singapore and Indonesia. Larger companies tend to have more awareness in a wide range of countries; smaller companies tend to be aware of regulations in two or three key markets.

In addition, most respondents mentioned being aware of restrictions in a small number of countries where they do not have business operations, such as China and Russia, due to their high profile and more restrictive nature.

Businesses reported that they use a number of sources in order to stay updated on data localisation policies changes, and these vary based on the size of the business. Large businesses typically have specialist in-house teams with responsibility for monitoring regulation and compliance, and often engage directly with governments on these issues, sometimes with a view to shaping policy. Smaller businesses were more likely to mention specific internet searches regarding the territories of interest to them, with some noting the importance of ensuring this information is from a trusted source such as a specialist law firm or a government website. A small number of businesses also noted receiving alerts and emails from the Information Commissioner's Office, which they find useful.

5.3.3 How data are stored and processed, and impacts of decisions

In-depth respondents reported a range of ways in which their businesses store and process data, partly in order to be compliant with data governance requirements, and the implications of these for data localisation.

Storing personal data

All businesses interviewed in depth store personal data, either on a small or large scale, and aim to be fully compliant with the country-specific regulations of their customers.

Modes of storage vary and include the use of cloud-based data centres, bespoke systems designed in-house or with partners (for larger businesses) and using "off-the-shelf" systems such as Microsoft Azure (for smaller businesses). This approach allows them to have access to data centres located in a range of territories, with businesses making strategic decisions about where they will be located in order to best meet their client's needs in the most cost-effective way while still being compliant with regulations.

Underpinning these decisions, most respondents noted the importance of standard contractual clauses and consent, ensuring their customers are aware of where their data is being stored. A small number of businesses which store data on behalf of clients, see it as the role of their client to advise and select where they want their data to be held, and to be compliant with a country's data localisation legislation and regulation.

Accessing and processing personal data

Several businesses experience more complexity when addressing the issue of accessing and processing personal data than they do with data storage – particularly where data are held in one location and those who require access are based in another.

As with data storage, strategic decision-making is frequently required to ensure compliance regarding who undertakes specific work and where they are based, and standard contractual clauses are also a key factor and enabler to facilitate client agreement.

In some instances, teams need to be established in-country to be able to accommodate data-processing requirements, both in large and small companies. However, some businesses noted they require and have established teams in these territories anyway, as they feel it helps them meet other regulations within a country and improve their ability to best service their customers – the adherence to data localisation considerations is an added benefit of this. However, one global company had found this approach frustrating as it meant that, in some instances, it was not able to utilise its global expertise when working in countries with strict data localisation policies.

In a few instances, businesses look to develop partnerships with companies in other countries to support data storage and processing. For some, this works effectively and is a cost-efficient way of ensuring a foothold in a particular territory. However, one company noted that it would have concerns about doing this following an instance of intellectual property (IP) theft from a partner.

Cost and implications of data localisation measures

Cost is the key factor in businesses' decision-making when making adjustments to adhere to data localisation requirements. Costs that may be incurred include direct costs such as infrastructure and personnel time costs, and wider indirect costs such as reduced opportunity for investment in resources and development of intellectual property.

The main direct cost discussed by larger businesses is the possibility of opening new data centres, which presents a significant investment both in terms of building and operational cost (particularly the cost of energy). One large business reported having been deterred by these costs when it explored this option in Indonesia, limiting its activity in this market.

Smaller businesses also discussed the cost of accessing new data centres, which present a fee to be paid to their providers. One smaller business noted that if a client required a new data centre to be established then it would need to pass on the cost of establishing this, which could result in it being less competitive.

After data storage, personnel time to investigate and implement changes was seen as the biggest direct cost when addressing data localisation requirements. Most respondents could not quantify the number of hours and associated costs this had involved and could potentially involve, but they felt it would be significant (including time to research requirements, review compliance, investigate adjustments needed to their approach and to enact any changes).

One business had also found that additional personnel and associated costs might be required when data localisation requirements meant it could not access the expertise of its global teams when processing personal data.

Other direct costs that businesses have expended to address data localisation requirements that were mentioned by a few respondents include costs to establish personnel and infrastructure in other territories and payments for expert legal advice (either in the UK or in the country of interest).

A small number of larger businesses also commented on the indirect impact which investing time and resources to respond to data localisation requirements had on their ability to invest in other aspects of their business. They believed this would have knock-on effects on their growth both in the UK and in other economies.

If a particular market or customer had specific data localisation requirements, most businesses would undertake a cost-benefit analysis, with the cost of compliance being weighed against the benefits of entering the market. As noted previously, where these costs were too high, it would prevent them from entering a specific market or would determine the extent and nature of entry into a market.

5.3.4 Adherence to legislation and regulations

All the businesses interviewed in depth have taken steps to ensure high levels of compliance with the data localisation legislation and regulations relevant for their customers, where they believe they are responsible for this (some businesses believe responsibility lies with their larger clients who make the decisions about how data is stored and processed). These steps include reviewing their existing processes for compliance and addressing any gaps in their practice, as discussed previously. Businesses' behaviour is in part driven by a combination of client expectation (which varies considerably – with business clients keen to establish and determine data protection requirements, and personal customers typically being confident in the structures in place to provide informed consent) and the desire to follow appropriate laws and avoid litigation or fines.

In keeping with this, in some instances, businesses have chosen not to expand into territories which are deemed either too costly or too risky. This includes China, some South American states and some African states. This resonates to some extent with the survey findings which suggest that respondents find legislation in these countries to be relatively opaque.

Some of the businesses interviewed in depth felt that exact adherence and compliance cannot always be determined, with some countries' guidance being described as vaguer than others. This therefore leaves much legislation open to interpretation which creates difficulties for businesses and a concern that they will be "caught out". A small number of businesses stated that they prefer more trust-based systems which provide appreciation of sufficient risk assessment and measures.

In addition, several respondents noted that some businesses have different attitudes and approaches to risk (of being fined or faced with other legislative action), which likely affect how they interpret and respond to data localisation

measures. This led to concerns of an "uneven playing field" where some competitors might benefit from being less risk averse.

Among respondents, attitudes to risk also varied. For example, one smaller company observed that its willingness to accept risk might be higher as it is likely too small to be of interest to countries seeking to enforce their policies, with larger companies more likely to be targeted here. Others which act as intermediaries in the supply chain believe the risk to be on their large client's side – as they are the ones acquiring customer data in the first place – when determining contractual terms and how data localisation measures are implemented.

Several respondents have found that the process to further clarify different countries' regulation can be complex, with requests for further information from regulators being slow, lacking response or providing a determination that does not work in a company's favour (Schrems II was cited by a small number of respondents as an example of this).

Further information from UK and other governments clarifying the specifics of different countries' policies would be welcomed by businesses, although some noted their preference would be something short and clear, based around the broad principles and clear "red lines" of different policies.

5.3.5 Impact of changing laws

Most of the businesses interviewed in depth (both large and small) were aware of the possibility of future restrictions in some countries, particularly in India, China and the USA. Some were of the view that there was generally an increasing trend towards data localisation, notably in financial services. For some countries, such as India, Indonesia and Vietnam, this is part of a wider trend towards more protectionist data policies. For others, such as China, it reflects the influence of national security objectives.

For some, this meant they were examining the likely costs that would be incurred in responding to specific policies and the risks inherent in different approaches (such as disproportionate investment of money and resources, increased threat of data risks and increased threat of IP theft). Some were also considering the possibility that they might be unable to do business in particular territories as a result of these risks.

A few businesses felt data localisation which has the effect of reduced presence in a country or increased cost would be detrimental locally, as they would not be able to invest in other ways (such as in infrastructure, innovation and staff development), and local businesses might not have as much choice for partner and support options.

Some larger businesses also expressed concern that further changes could be highly detrimental for smaller businesses which might not have the ready finance and support to be able to respond accordingly.

A small number of businesses noted that understanding the underlying motivations of different governments' data localisation policies was key in resolving real-world challenges and implications in implementing them. As such, several of the larger businesses interviewed in depth reported that they engage directly with

governments and via trade bodies and membership organisations in order to effectively lobby policy-makers to share their views in a coordinated manner. This has the dual benefit of having additional advocacy support and ensuring they continue to maintain positive relationships with policy-makers.

Several businesses stated that they would find alerts and information from government sources helpful if they contained specific information on the implications of any changes and what this means for businesses in practice. One respondent from a large business noted that it can be challenging to keep up with regular changes to draft policy. Their preference would be to find out the final agreements and implications of a policy so they can adapt accordingly during the implementation lead-in time, rather than preparing for hypothetical situations which could be costly for smaller businesses.

Some interviewees also pointed to a disconnect between the way in which authorities approach data governance and the way business operations are conducted. For example, the Indian government is considering a distinction between personal data and critical personal data, the latter being subject to more restrictions. However, businesses which provide platform and network services do not necessarily segment data in that way.

Recognising that differences between countries in approaches to data governance could restrict cross-border data flows, some of the larger businesses interviewed discussed possible approaches for how differences between countries on data governance could be managed. A few favoured a multilateral approach which provides internationally developed standards that companies and countries across the world can follow and abide by, making it more straightforward to do business. Others favoured regional models, such as the GDPR, which harmonise approaches across a range of countries, and which could be extended through bilateral instruments. Others believed bilateral agreements were more likely to be effective, using trust-based models similar to recent agreements between the UK and Japan, which were welcomed as examples of effective practice. A small number of respondents believed that the UK is well placed to drive this agenda and good practice regarding data flows as it continues to make trade agreements following its exit from the EU.

5.3.6 GDPR (role, recognition, treatment)

Businesses which responded in depth were very aware of GDPR and most had made considerable changes to their data storage and processing approaches ahead of its implementation, for example by establishing additional data centres in Europe and reviewing contractual clauses with clients.

They believed that, while it was challenging to implement at the time, GDPR could now be considered a “gold standard” for data protection, with high levels of awareness of the regulation across the world. This tallies with findings from the YouGov survey. For many, the assurance that they and their partners are acting in accordance with GDPR is a reassuring factor for their clients, and most companies expect their partners to abide by it even if it is not in effect in their country.

Some businesses felt that GDPR helps to create a level playing field as a default privacy standard. However, others noted that where countries and businesses may

not subscribe to GDPR this could lead to challenges whereby some may simply ignore it as ease of access to data and speed are more important.

5.4 Synthesis of qualitative findings

Comparing the results from the different strands of qualitative research is hazardous given the differences in sample size and the self-selecting nature of the businesses involved in in-depth interviews. However, taking these factors into account, one of the trends that seems to emerge is a "sorting" between businesses that are data aware and data unaware. This does not necessarily seem to be a function of size, as demonstrated by the survey results although, clearly, as revealed through the interviews, large global players are not only aware of data policy but actively try and shape it. Moreover, while some interviewees were able to point to significant investments in data strategy to ensure compliance and optimise operations around it, the majority of respondents did not agree that such investments were strategically significant.

This sorting suggests that there is a significant block of businesses whose operations are data enhanced and that could be exposed to sudden shifts in data policy and/or effects of more stringent enforcement. This in turn could suggest that the negative impacts modelled in section 4 could understate the true impacts of localisation.

5.5 Business research summary

Together, the findings from the YouGov survey and the qualitative interviews provide valuable insights on the level of awareness and impact of data localisation measures among British businesses.

As noted in the previous section, these findings are not directly comparable, given the differences in sample size, differences in the way in which responses were collected across the two strands and the self-selecting nature of businesses involved in in-depth interviews. However, bearing these factors in mind, we note some of the key complementarities and differences across the findings from the two strands below.

Impact of changing laws

Across both strands (YouGov survey and in-depth interviews), there was some consensus across businesses that changes in laws towards data localisation would likely have a detrimental impact. The YouGov survey results highlighted that over 50% of businesses which export goods and/or services to the listed countries believed they would be negatively impacted if countries that their business operates in required that all personal data from clients and employees in those countries had to be stored exclusively in those countries.

Across businesses which were interviewed, some felt data localisation which had the effect of reduced presence in a country or increased cost would be detrimental locally. Larger businesses also expressed concern that further changes could be highly detrimental for smaller businesses.

Awareness of data localisation requirements for countries of export

The survey results found that businesses' awareness of country-specific requirements around storing or transmitting data to countries was relatively limited, with over a third of businesses which import or export goods or services in the listed countries and hold personal data stating they were not aware of the nature of the country-specific requirements or indeed whether these requirements exist. However, in contrast, the in-depth interviews found that respondents from both large and small companies were aware and mindful of data localisation requirements in the countries in which they operate and use a number of sources in order to stay updated on changes to data localisation policies.

To some extent, this variation in findings may be explained by differences in the nature of the business samples. While the survey responses on questions related to awareness of requirements cover businesses which import/export in the listed countries, this does not provide an indication of the level of engagement/importance of exports and data localisation for these businesses. To the extent that these are not key activities for some of the businesses surveyed, we might expect this to reflect in their levels of awareness of such requirements. However, for all respondents of the in-depth interviews, it is clear that the ability to store, transfer and/or process personal data is itself a key business activity or plays a critical function facilitating business operations.

Recognition of the role and importance of GDPR

Across both the qualitative strands, GDPR was broadly recognised as the key regulation on data protection. According to the survey results, over 56% of businesses recognise GDPR as the highest standard of data protection and close to 70% of businesses stated they apply GDPR guidelines as a standard across all countries they operate in, even where GDPR is not a requirement in these countries.

The businesses interviewed were also very aware of GDPR and most had made considerable changes to their data storage and processing approaches ahead of its implementation. They believed that, while it was challenging to implement at the time, GDPR could now be considered a "gold standard" for data protection, with high levels of awareness of the regulation across the world.

6 CONCLUDING OBSERVATIONS

The research in this report has highlighted the economic importance of cross-border data flows to the UK, and a number of its major trading partners. That economic importance can be assessed in a number of different ways. This report has focused on one particular channel of impact: via international trade. The approach is intuitive given the role played by cross-border data flows as a facilitator of international trade. Restrictions act as an implicit tax on trade, and specifically on sectors that are data-intensive.

There are signs that the international policy landscape for cross-border data flows is becoming more restrictive. This in part reflects a willingness by governments to pursue broader public policy objectives by imposing conditions that need to be met if cross-border data flows are to be substantially liberalised. Some jurisdictions are also pursuing or maintaining measures that impose absolute restrictions on cross-border data flows.

All economies stand to suffer substantial economic losses from increased restrictions on cross-border data flows. With the exception of China (which is already highly restrictive in its approach to cross-border data flows), GDP losses lie between 1.5% and 2.5% per year, if all major countries were to adopt fully restrictive policies on cross-border data flows. The UK is at the upper end of this range, reflecting the importance to it of a number of major data intensive sectors.

The results underscore the value of international collaboration in maintaining a low level of restrictions on cross-border data flows, and finding ways to ensure that wider public policy objectives are pursued through means that are no more restrictive on trade than necessary. Such collaboration can take the form of provisions in Free Trade Agreements (FTAs), arrangements negotiated under the auspices of the WTO (such as the current Joint Statement Initiatives) and in bespoke bilateral data agreements. By and large, the virtue of these provisions is to help lock-in existing levels of liberalisation, and thus to avoid the nefarious effects reported above of an upsurge in localisation. Moreover, by providing greater certainty, the locking-in effect can also facilitate efficient investment decisions. Finally, the agreements could also set the stage for deeper collaboration between partners.

ANNEX A MODELLING APPROACH

The modelling approach is to represent changes to data localisation as changes to the OECD's Services Trade Restrictiveness Index (STRI) in terms the parts of it that relate to data localisation. This is combined with estimates of the responsiveness of trade to the STRI, which is calculated in a gravity model. This is used to calculate changes to trade on a bilateral, sector-level basis. For example, we model separately how changes to data would affect telecoms trade between the UK and USA, UK and India, UK and Argentina, etc. These impacts are then added up across trading partners and countries to give overall trade impacts by scenario.

The analysis focuses on data "intensive" sectors. This includes core sectors such as computing and telecoms, which include data-enabled industries, as well as sectors that draw heavily on these inputs. In addition to services sectors, we include high-value manufacturing, which reflects the role of data through integration of services and goods such as software in cars.

This section provides further detail on various aspects of the modelling approach:

- The Services Trade Restrictiveness Index
- Services trade gravity modelling
- High-value manufactured goods gravity modelling

Services Trade Restrictiveness Index

The STRI assesses how restrictive a jurisdiction is to foreign services providers, with a value of zero meaning completely open and a value of one meaning completely closed.

Barriers to services trade are defined in terms of:

- Restrictions to foreign entry
- Movement of people
- Discriminatory measures
- Barriers to competition
- Regulatory transparency

The STRI is calculated using a scorecard containing a long list of restrictions pertaining to the above categories. Each of the restrictions carries a weight and, if in place, the corresponding weight[47] is added to the score. If all of the restrictions were in place, the weights would sum to one and the jurisdiction would be seen to be completely closed.

The STRI incorporates five restrictions ("lines") which describe the stance in relation to cross-border data flows. This sits within the "restrictions to foreign entry" category. The five restrictions are:

[47] The weights attached to restrictions reflect the consensus view of sector experts.

- Cross-border transfer of personal data is possible when certain private sector safeguards are in place;[48]
- Cross-border data flows: cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws;
- Cross-border data flows: cross-border transfer is subject to approval on a case-by-case basis;
- Cross-border data flows: certain data must be stored locally; and
- Cross-border data flows: transfer of data is prohibited.

Each of the five lines carries the same weight, but the weights vary by sector, reflecting the relative importance of data. In computer services, each line carries a weight of 0.014. This means that moving from having none of the data restrictions in place to having all five in place would increase the STRI by 0.07.

The overall modelling approach is to simulate the impact on trade of turning these restrictions "off" or "on". In the UK, and many relatively liberalised countries, typically one line in five of the restrictions is "on".

Scenarios

In the first scenario we consider the effect of both trading partners moving from current restrictiveness to full restrictiveness by taking the current data flow restrictions that are "on" and moving to having all five of the lines on. The change in the STRI is therefore given by taking the number of lines being switched on and multiplying by the weight, which is calculated separately for each sector. This can be written as follows:

$$\Delta STRI = (5 - STRI\_lines\_current\_c\_s) \times Weight\_s$$

for sector s and country c.

As we shall see, both the exporter's and importer's STRI affect trade, so the modelling looks at how both of these STRIs are changing.

The responsiveness of trade is calculated in a proportional manner, so one country changing STRI produces a percentage change in trade, as does any change in STRI by the partner country.

The second scenario looks at the incremental benefit, relative to scenario 1, of entering into reciprocal arrangements with EU that secure liberalised flows of cross-border data. We assume that, for trade with the EU, instead of moving to having all five lines of restrictions, we move to having one ("Cross-border data flows: cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws").

For the UK, which currently has one line in most sectors, this represents little movement from the status quo vis a vis the EU, but it is considerably more liberalised than the full restrictiveness modelled in scenario 1. For more restrictive jurisdictions such as China or India, this represents considerable liberalisation.

[48] A "NO" to this line is considered restrictive, whereas a "YES" is considered restrictive in the other four lines.

We now describe the gravity modelling, which is used to estimate the sensitivity of trade to changes in the STRI. Due to the different characteristics of goods and services and how they respond, as well as coverage in different datasets, the two are modelled separately.

Services trade gravity modelling

The effect of services trade restrictiveness on trade flows is estimated using a gravity model. This largely follows the approach pursued by the OECD STRI analysis.[49]

The gravity model predicts services trade flows as a function of distance, GDP, common language, contiguity, colonial relationship, STRI scores of exporting and importing countries (relating to the sector in question), and whether the trading pair are both in the EU.

The aim is to generate elasticities for the STRI that will estimate how changes to the value of STRI affect bilateral flows between the UK and the US.

Data

The main dataset, including distance, GDP and dyadic variables, is from CEPII.[50]

Bilateral services trade data is from OECD EBOPS[51] and is reported for a number of different sectors. The STRI is also from the OECD[52] and the dataset used here covers the years 2014-16.[53]

The following sectors have both STRI and trade flow data available, and are incorporated in the model:

- Sea transport
- Air transport
- Other modes of transport
- Postal and courier services
- Construction
- Insurance and pension services
- Financial services
- Telecommunications services
- Computer services

[49] Nordås and Rouzet "The impact of services trade restrictiveness on trade flows", Hildegunn K., The World Economy (2016).

[50] http://www.cepii.fr/cepii/en/bdd_modele/presentation.asp?id=8, dataset originally developed for Head, K., T. Mayer AND J. Ries, (2010), "The erosion of colonial trade linkages after independence", Journal of International Economics, 81(1):1-14.

[51] https://stats.oecd.org/Index.aspx?DataSetCode=TISP The TISP dataset covers modes of supply 1 (cross-border supply), 2 (consumption abroad) and 4 (movement of natural person). It does not capture mode 3 (commercial presence).

[52] http://stats.oecd.org/Index.aspx?DataSetCode=STRI

[53] It should be noted that although the dataset is technically a panel, there is little variation in STRIs over time, which means there is very little scope to use the panel aspect of the data, such as with fixed effects. Therefore the cross-sectional aspect of the data drives the results, and one-year pure cross-section models generate very similar results.

- Legal services
- Accounting, auditing, bookkeeping and tax consulting services
- Architectural services
- Engineering services
- Audio-visual and related services

Note that for audio-visual, although STRIs are provided separately for broadcasting, motion pictures and sound recording, the trade flow data are only broken down as for audio-visual, with no further disaggregation available. Therefore the gravity modelling includes the audio-visual sector as a whole with the STRI values averaged across the three sub-sectors.

The range of countries covered is constrained by the availability of STRI data. As with OECD, the STRIs are calculated for Brazil, China, Colombia, Costa Rica, India, Indonesia, Lithuania, Russia and South Africa.

It is important to note the limitations of the services trade data. In particular, there are many gaps in the published TISP data, for example, due to data being redacted for confidentiality reasons or not split out into detailed sectors. In these situations, the gaps in the data can be addressed using "mirror flows". For example, if the UK does not report imports from Germany, we can instead use Germany-reported exports to the UK. However, for whatever reason, the trade flows reported by the exporter are generally larger than the same flows as reported by the importer. Therefore, to "infill" the data, we first estimate importer-reported flows using exporter-reported flows, derive the predicted values, and use these where the importer-reported trade flows are missing.

Specification and results

The regression is estimated using a poisson pseudo-maximum likelihood (PPML) approach, following the Nordas-Rouzet paper. The coefficients in a PPML regression give the proportional change in the dependent variable in the same way as in an ordinary least squares (OLS) regression with a logged dependent variable[54] The PPML approach is argued to be better for dealing with missing observations and is described in detail in Silva and Tenreyro.[55]

We predict trade from country I to country J as a function of size of the two countries (log GDP), the STRI scores of the two countries, a series of dyadic variables X (log distance and dummies for common language, contiguity, colonial relationship and whether EU pair), year dummies and sector dummies.

This can be written as follows:

$$\text{Trade flow}_{ijst} = b_0 + b_1 \text{logGDP}_i + b_2 \text{logGPD}_j + b_3 \text{STRI}_i + b_4 \text{STRI}_j + b_5 X_{ij}$$
$$+ b_6 yr_t + b_7 \text{sector}_s + u_{ijst}$$

The results of the pooled regression are shown in Figure 57 below. The first column includes all 14 sectors for which STRI data are available. The exporter STRI

[54] In a PPML model, the coefficients give a proportional change in the dependent variable. In both cases, the percentage change in the dependent variable for a change in variable X is given by exp(βvar*Δvar)-1.

[55] The Log of Gravity, Review of Economics and Statistics, 2006. The authors use Monte Carlo simulations to compare the performance of log-linear OLS and PPML estimators.

coefficient of -1.53 means that if the score is reduced by 5 percentage points, trade will be increased by 8%.[56] The other coefficients, e.g. on gross domestic product (GDP) and distance, are comparable to other services trade gravity model estimates. The second column shows results relating to the nine sectors most comparable to the sectors of interest, focusing on communications and professional services (transport, logistics and construction are excluded). The STRI coefficients become somewhat larger. The third column shows results for the physical sectors. Here the coefficients are smaller and the importer STRI is statistically insignificant.

Figure 57 Services trade regression results

	Pooled model	Digital sectors	Distributive sectors
Log distance	-0.591	-0.666	-0.541
	[22.29]**	[14.47]**	[-22.47]***
Log GDP exporter	0.548	0.604	0.494
	[39.78]**	[26.72]**	[32.69]***
Log GDP importer	0.612	0.61	0.618
	[33.61]**	[18.79]**	[37.14]***
Contiguity dummy	-0.022	-0.293	0.220
	[0.37]	[3.05]**	[3.34]***
Common language dummy	0.544	0.781	0.287
	[8.16]**	[7.53]**	[3.81]***
Colonial dummy	0.417	0.437	0.357
	[5.27]**	[3.90]**	[3.32]***
STRI exporter	-1.535	-2.441	-0.626
	[6.51]**	[5.49]**	[-2.59]***
STRI importer	-0.923	-1.718	-0.249
	[5.22]**	[6.12]**	[-1.1]0
EU pair	0.133	0.157	0.102
	[2.54]*	[1.71]	[1.94]*
Constant	-21.9	-27	-21.317
	[33.0]**	[23.9]**	[-29.1]***
R2	0.28	0.24	0.38
N	39232	24977	14255

Source: Frontier analysis of OECD and CEPII data.

*Note: T-statistics in parentheses, significance levels:***p<0.01 ** p<0.05; * p<0.01.*

Choice of control variables

As the sample is relatively small, care is needed in terms of the control variables that can be included together in the model. They may be highly correlated with each other, which may cause some of them to take a counterintuitive sign, for example. We therefore undertake a model selection approach to retain a limited number of variables which do not give counterintuitive results. For example, while we find that an EU dummy has a moderate positive impact, including a generic FTA dummy causes the EU dummy to get larger but the FTA dummy has a negative sign, the STRI variables stay the same. Meanwhile the FTA dummy can change sign depending on the inclusion of other variables. We therefore exclude the FTA dummy as there is essentially not enough variation in these data to pick apart the relative effects of different types of FTA alongside the effects of the STRI.

[56] Using the marginal effects formula above, this is given by Exp(-1.53*-.05) -1 = 8%.

We also explored supplementing the model with intra-EEA STRIs. In theory, these should have the benefit of offering more precise bilateral measures of restrictiveness, whereas the standard STRI is reported on a most favoured nation (MFN) basis. They could therefore be included to explore the effects of bilateral deviation from the MFN level. However, we again find that these variables take a positive sign, i.e. so that having less restrictiveness vis a vis the partner trading relative to MFN levels results in lower trade than would otherwise be the case. This result is counterintuitive, and we suspect it arises because there is insufficient variation in the data to be able to reliably pick apart these effects.

Pooled regressions

The limited variation in the data gives a strong justification for using a pooled regression, as cutting the data too is seen to give overfitted models with counterintuitive results. In a pooled regression, the intercept (sector) dummies control for the average sizes of sectors (e.g. telecoms is larger than audio-visual). Meanwhile, the coefficients estimated for the STRI, the dyadic variables and GDP are constrained to be the same across sectors. This exploits the maximum amount of information in estimating an average STRI effect.

The alternative to a pooled approach is to run separate regressions for each sector in turn, which is explored in Nordas and Rouzet. This gives a much larger range of STRI coefficients, with some becoming very large and others taking on a counterintuitive sign.[57] This amount of variation in the parameters is implausible and not consistent with prior empirical evidence on their effects. While there may be some genuine sectoral variation in responses to the variables (e.g. sea freight is less responsive to distance than terrestrial transport), it is not obvious, for example, why architecture should be much less responsive to distance than engineering or legal services are. This suggests that the sector-level regressions are overfitted and that the pooled results are to be preferred. On this basis, we consider that the pooled sub-sample results are reasonable, as they use the maximum amount of variation available in the data by drawing on trade relationships for similar sectors and are less prone to influence from quirks in the data.[58] For similar reasons, we seek to run regressions on the maximum sample of countries rather than on subsets of them, which again causes the coefficients to become less stable.

Goods trade gravity modelling

We hypothesise that “high-value manufacturing” is particularly sensitive to services inputs, of which data flows are a component. We therefore wish to estimate a model in which trade flows in these goods are the dependent variable.

We extend the analysis by estimating a gravity model of goods in which we include measures of services trade restrictiveness to allow us to derive the impacts of data

[57] For example, banking has an elasticity of -13 while road has a positive sign.

[58] For a broader discussion of pooling, refer to the following papers. Baltagi, B.H. & J.M. Griǿ n (1997), “Pooled Estimators versus their Heterogeneous Counterparts in the context of dynamic demand for gasoline”, Journal of Econometrics, 77: 303-327.

Baltagi, B.H,.J.M. Griǿ n & W. Xiong (2000), “To pool or not to pool: homogeneous versus heterogeneous estimators applied to cigarette demand”, Review of Economics and Statistics, 82: 117-126.

localisation measures proxied for by changes to the STRI. In this respect it follows the services trade analysis. There are two key differences: first, there may be additional drivers that affect the goods trade and not services; second, sector-specific STRIs cannot be linked to trade flows at the sector level in the same way as can be done for services. A further complication is that some of the relevant variables for the dataset are captured at different points in time and it is difficult to compile a genuinely contemporaneous dataset.

Data

The goods trade data are extracted from UN Comtrade using product codes that correspond most closely to high-value manufacturing.[59] We extracted data for 2019. In addition to the variables used elsewhere, it is considered appropriate to control for conventional barriers to the goods trade. The main indicator here is the Overall Trade Restrictiveness Index (OTRI) estimated by Kee et al.,[60] which measures the effect of tariff and non-tariff barriers to the goods trade. The problem is that these data were last estimated in 2012, and more recent indices for the goods trade are not available. As before, the dataset uses other controls from CEPII.

Note that as we use the STRI as control variable, this limits the number of countries that can be included in the regression, which is smaller than might often be used in goods analysis.

Analysis

Again, we undertake a parsimonious approach to variable selection, looking to retain variables that have a statistically significant and sensible interpretation. However, the overarching problem with the dataset is that it either omits or poorly measures the effects of tariff and non-tariff barriers to trade.

A further point to note is that China acts as a distortive outlier in the sample. It is a restrictive jurisdiction but has much higher than expected levels of goods and manufacturing trade than is predicted by the model. When included, many of the restrictiveness variables take on the "wrong" sign. On this basis, China is excluded from the sample.

Results

The first specification shows that both importer and exporter STRIs have a negative effect on trade in high-value manufactured goods. However, the exporter term is statistically insignificant. The second specification adds in the OTRI term. This results in slightly larger STRI coefficients. However, the OTRI term itself has the wrong sign, which raises concerns about how well it measures goods restrictions, which is unsurprising given it is potentially out of date.

[59] The following HS codes are used: 28 inorganic chemicals; 29 organic chemicals; 30 pharmaceuticals; 37 photographic / cinematographic; 38 chemicals n.e.c.; 85 electrical machinery / equipment; 86 railway locomotives; 87 vehicles; 88 aircraft; 90 optical / medical instruments; 91 clocks / watches; 92 musical instruments; 93 arms and ammunition.

[60] https://www.researchgate.net/publication/23646050_Estimating_Trade_Restrictiveness_Indices

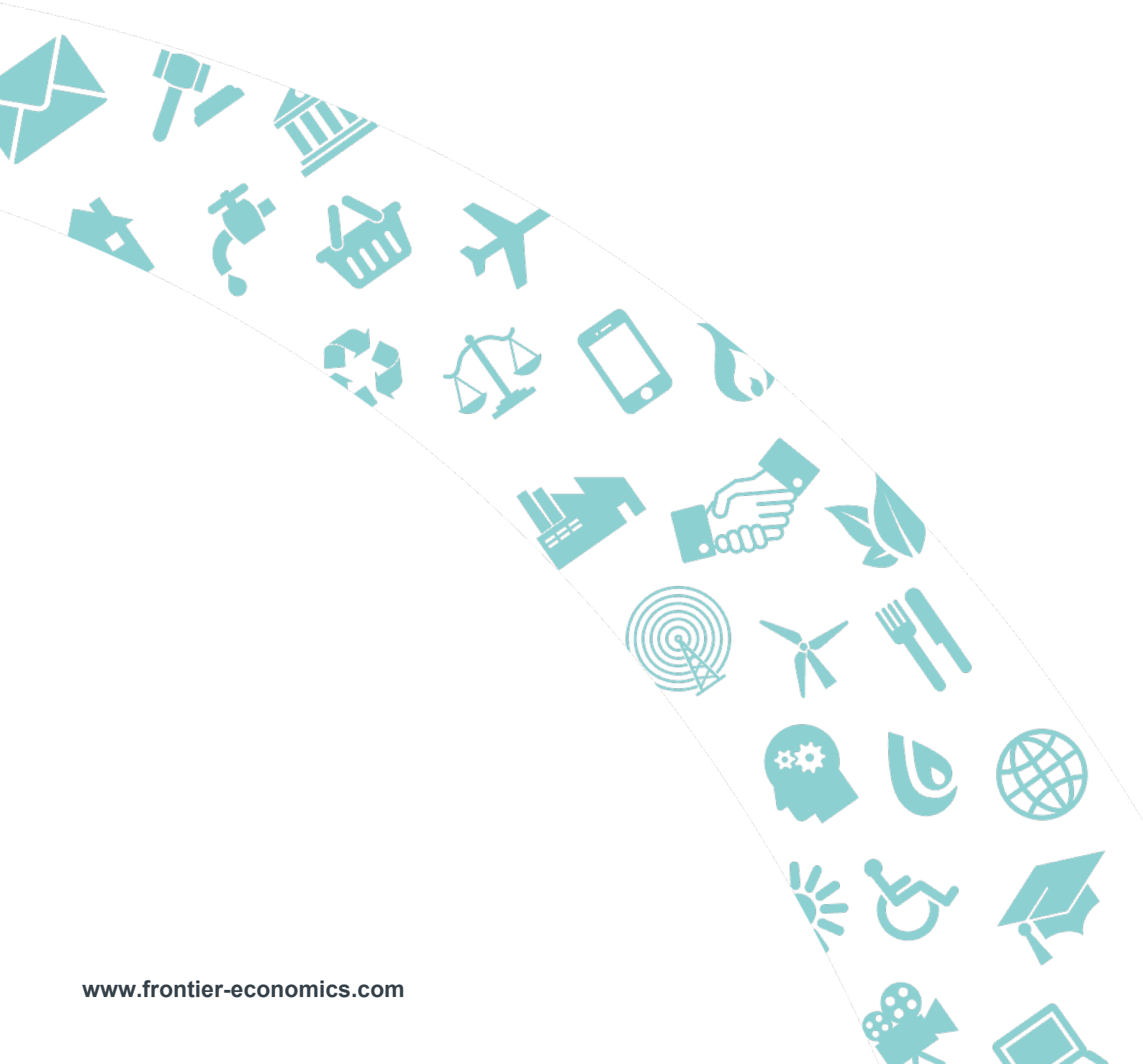
Figure 58 Gravity model with high-value manufactured goods

Variable	Specification 1 beta value [note a]	Specification 2 beta value [note a]
STRI exporter	-1.074 [0.886]	-1.348 [0.767]*
STRI importer	-0.946 [0.476]**	-0.965 [0.501]*
FTA dummy	0.154 [0.149]	0.154 [0.151]
EU dummy	0.414 [0.153]***	0.417 [0.158]***
Log distance	-0.367 [0.097]***	-0.383 [0.088]
Log GDP exporter	0.804 [0.035]***	0.802 [0.036]
Log GDP importer	0.905 [0.066]***	0.902 [0.062]***
Common language dummy	0.425 [0.148]***	0.423 [0.147]***
Time difference	-0.080 [0.041]**	-0.076 [0.038]**
Colonial dummy	-0.475 [0.186]**	-0.465 [0.187]**
Importer OTRI	-	0.19 [1.028]
Exporter OTRI	-	1.128 [1.927]
Constant	-10.633 [2.385]***	-10.397 [2.225]***
R-squared	0.61	0.61
N	1979	1979

Source: Frontier analysis of OECD, Comtrade and CEPII data.

*Notes: [a] T-statistics in parentheses, significance levels: ***p<0.01 ** p<0.05; * p<0.01.*

frontier economics



www.frontier-economics.com