Bauer, Matthias; Ferracane, Martina F.; Lee-Makiyama, Hosuk; Van der Marel, Erik

Research Report

Unleashing internal data flows in the EU: An economic assessment of data localisation measures in the EU member states

ECIPE Policy Brief, No. 3/2016

Provided in Cooperation with:
European Centre for International Political Economy (ECIPE), Brussels

Suggested Citation: Bauer, Matthias; Ferracane, Martina F.; Lee-Makiyama, Hosuk; Van der Marel, Erik (2016) : Unleashing internal data flows in the EU: An economic assessment of data localisation measures in the EU member states, ECIPE Policy Brief, No. 3/2016, European Centre for International Political Economy (ECIPE), Brussels

This Version is available at:
http://hdl.handle.net/10419/174802

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

POLICY BRIEF

No. 03/2016

Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States

by Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, Erik van der Marel

EXECUTIVE SUMMARY

- Forced data localisation measures are on the rise around the world, fragmenting the Internet and increasing costs for businesses and consumers. Until the year 2000, only 15 measures were imposed globally. By 2007, the number of measures doubled and it more than doubled again until today.

- The study has identified 22 data localisation measures where European Union Member States impose restrictions on the transfer of data to another Member State. The most common restrictions target company records, accounting data, banking, telecommunications, gambling and government data. In addition, there are at least 35 restrictions on data usage that could indirectly localise data within a certain Member State.

- A real EU Single Market on data storage is yet to come into function in practice: Two-thirds of all demand for "ICT-related" services (consulting, hosting, development) are sourced locally within each Member State, while only 18% is sourced from the rest of the EU. Meanwhile, the cost difference of operating data centres can be considerable amongst the EU Member States, with the most expensive country being twice as expensive as the cheapest.

- Data localisation measures create a major misallocation of resources and threaten the continent's productivity and competitiveness. If data can be stored and processed anywhere within the EU, the move would boost the commitment to achieve a true Digital Single Market and send a clear political message that Europe is open for business.

- If existing data localising measures are removed, GDP gains are estimated to up to 8 billion euros per year (up to 0.06% of GDP), which is on par with the gains of recent free trade agreements (FTAs) concluded by the EU. These gains approximate the impact of a fully price-transparent "industrial" DSM.

- Even more striking gains from a ban on data localisation will stem from the ratchet effect – preventing EU Member States from imposing harmful data localisation measures in the future. The economic loss generated by full data localisation by each of the Member States would lead to a loss of EU-wide output by 52 billion euros per year (0.37% of GDP). This number will increase with further digitalisation of the European economy.

BACKGROUND[1]

The online environment has rapidly become one of the most regulated areas of social and commercial interactions, often surpassing their traditional offline counterparts. Whether the objective is to protect personal data, tax revenues, or essential infrastructure, the sovereign is increasingly active in seeking continued jurisdiction over online activities of their citizens and firms. At times, it is not acting to fill a legal void but using disproportionate means to repatriate consumers and firms who use the internet to trade with or from other countries.

Perhaps one of the most draconian measures is data localisation, where governments are requiring mandatory storage of critical or trivial business data on servers physically located inside their territory. Whether the pretext is "restoring confidence" in the online commercial environment – or just plainly to "level the playing field" between domestic players and foreign competitors – data localisation effectively disrupts cross-border data flows and consumer access to online services. Meanwhile, production chains are increasingly digitalised. Even trade in goods and hard commodities – from cars to raw materials – depend on data access;[2] various types of consumer services that were considered "untradeable" less than a decade ago are now exchanged online.

As the global policy environment inclines towards "data nationalism", data localisation has become an effective non-tariff barrier (NTB) to trade (Chander, Lê, 2014). Previous literature established also that data localisation result in clear economic costs for the implementing economy, primarily through significant losses in productivity and competitiveness.[3] Europe – as an export-led services economy under considerable competitive pressure – stands more to lose from such losses. Meanwhile, data localisation measures rarely contribute to their alleged policy objectives, as information security is not a function of where the data is physically stored.

Intra-EU Dimensions on Free Flow of Data

Whereas there are strict restrictions on data flows from the EU to other countries,[4] there are fewer restrictions imposed on internal flow of data between EU Member States thanks to the existing Single Market disciplines on services.[5] Nonetheless, a real Single Market on data storage is yet to come into function in practice: Two-thirds of all demand for "ICT-related" services (consulting, hosting, development) are sourced locally within each Member State, while only 18% is sourced from the rest of the EU.[6]

The policy package under the Digital Single Market (DSM) includes consumer-driven initiatives such as a European Cloud as well as the prevention of "unjustified" geo-blocking as well as cross-border content portability.[7] To augment DSM with a ban on "unjustified restrictions on the location of data for storage or processing purposes" as envisaged,[8] would create an industrial dimension to free flows of data, which the DSM strategy currently lacks.

[1] ECIPE gratefully acknowledges the support for this paper from Computer & Communications Industry Association Europe (CCIA Europe).
[2] See Rentzhog, 2014; 2015.
[3] Notably ECIPE, 2014; 2015; US Chamber of Commerce, 2013.
[4] General Data Protection Regulation 2016/679 (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC).
[5] Inter alia Articles 26 (internal market), 49 to 55 (establishment) and 56 to 62 (services) of the Treaty on the Functioning of the European Union (TFEU) and Services Directive (Directive 2006/123/EC on Services in the Internal Market).
[6] WTO-OECD, Trade in Value Added (TiVA) Database, 2015.
[7] European Commission, Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC, COM(2016) 289 final 2016/0152 (COD); on ensuring the cross-border portability of online content services in the internal market, COM(2015) 627 final 2015/0284 (COD).
[8] European Commission, VP Ansip, A Digital Single Market Strategy for Europe, SWD(2015) 100, 6 May 2015.

The policy context for such intra-EU discipline on data localisation measures is favourable and timely. An EU-wide discipline against data localisation that would not impair on the protection of personal information – and given the passing of General Data Protection Regulation (GDPR) ought to be depoliticised, or to the extent the issue could ever be in the European discourse. A data localization ban would not change or affect the privacy rules under GDPR, which already asserts free flow of personal data within the EU.[9] Indeed, the current window of opportunity allows the EU to act before the EU Member States enact measures that could hurt other Member States and further fragment the Single Market.

The policy is also a matter of public communication: Despite the efforts of DSM (supplemented even by fiscal measures), the business is not yet fully convinced about the investment climate in Europe. Tech investment in Europe is rapidly catching up, reaching $8bn per year – [10]which is still less than half of what Silicon Valley attracts from venture capitalists alone. A ban on data localisation measures is not only a guarantee that innovators of cloud technologies, big data and other new innovations are able to gain ground and scale up within Europe – it would also restore some of Europe's credibility as a force to keep the global markets open. If the EU Member States follow the global trend towards data nationalism, then the DSM and the Single Market would have very little value in practice.

An economic assessment of policies on the digital economy are perilous endeavours, fraught with several methodological issues. This study builds on the methodology developed by the authors, which is accepted on methodological grounds,[11] using a computable general equilibrium (CGE) model, which is a well-acknowledged methodology that is frequently used for trade and economic impact assessments by academia and policymakers worldwide as well as the European Commission.[12] The impact of intra-EU data localisation is estimated in two parts: Firstly, the study looks at the liberalisation of existing regulatory data localisation measures (outlined in section two), given that the measures are also reasonably actionable. In addition, the study looks to the impact of economy-wide data localisation requirements imposed by each of the EU Member States to estimate the nominal economic damage that a data localisation ban would prevent.

1. EU REGULATORY FRAMEWORK ON FREE FLOW OF DATA

Access to foreign markets through trade liberalisation and globalised supply chains are major sources of growth, job creation and new investments. Given the nature of today's interconnected economy, Member States' policies that increase data storage and processing costs have an economic impact beyond telecoms and the internet. Manufacturing and exports are already, and increasingly, dependent on having access to a broad range of services at competitive prices – such as logistics, retail distribution, finance or professional services, which in turn are heavily dependent on secure and efficient access to data across a reasonably large area. When data must be confined within a Member State (that are mostly small or mid-sized economies), it does not merely affect internet-related services, but potentially any business that uses the internet to produce, deliver, and receive payments for their work, or to pay their salaries and taxes.

Many current restrictions are non-regulatory in nature, i.e. organisational decisions by individual firms rather than laws. For example, a bank or a public hospital may decide that its application vendors must store all its data on the premises, although there are no such obligations legally. However, the scope of this study is on those regulations which affect cross-border flow of data within the Single Market – in other words, law and decrees that blocks data transfers internally within the EU.

[9] See note 4.
[10] Dow Jones Venturesource, 2015.
[11] van der Marel et al., 2015 and Bauer et al., 2014.
[12] See, e.g., Economic Impact Assessments conducted by Francois, 2013 and 2007.

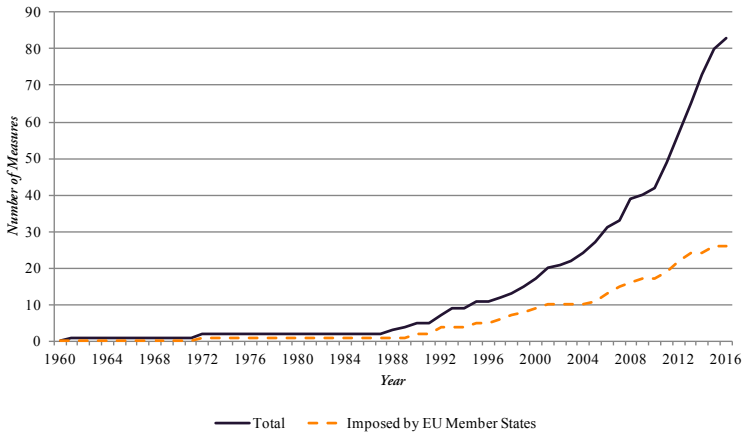
Many of today's restrictions are related to what certain EU Member States consider to be its vital national and fiscal interests, and uneasiness about data not being made available to its law enforcement or tax authorities upon request. Given that outright blockages to transfer of data would contravene EU's Four Freedoms and existing EU disciplines,[13] several of today's intra-EU restrictions relate to the national security exception,[14] granting national security as "a sole responsibility of each Member State". However, the Court of Justice of the European Union (CJEU) has reiterated in several rulings that such exception should be applied strictly and that the Member State requesting such exception should "prove that is necessary to have recourse to that derogation in order to protect its essential security interests".[15] While data localisation measures relating to public security, defence and state security clearly fall outside of the scope of EU law, such objectives cannot be used routinely or carte blanche to get out of Single Market commitments.[16]

Another policy objective for localisation relates to data protection. The EU has a common set of data protection rules since 1995. In recent months, the GDPR was adopted by the European Parliament and will enter into force by mid-2018. Given the harmonisation of privacy legislation across the EU under the GDPR, privacy can no longer be a concern for intra-EU data flows. The current and coming data protection regime in the EU remains quite diverse, yet – at least on paper – data should be allowed to flow freely within the Single Market. Nonetheless, Member States have imposed a series of additional requirements – most of which predate the 1995 European Data Protection Directive.

2. MAPPING EXISTING DATA LOCALISATION MEASURES IN EUROPE

Those regulatory regimes for which data is required to remain within a certain jurisdiction - and therefore cannot cross the border - are defined as data localisation or data residency requirements. The last decade has seen a worrying increasing trend of data localisation worldwide (Figure 1).

Figure 1: Number of data localisation measures implemented globally and intra-European Union



Source: ECIPE Digital Trade Estimates, 2016.

The oldest measure – which actually pre-dates the internet, but is enforced online – was implemented as early as 1961. Until the year 2000, only 15 measures were imposed globally. By 2008, the number of measures doubled and it more than doubled again until today.

[13] See note 5.
[14] Art. 4 (2) TFEU.
[15] See ECJ, *European Commission v Italy*, C-239/06, 15.12.2009, para 50; *ZZ v UK Secretary of State of the Home Department*, C-300/11, para 61, 4.6.2013.
[16] *European Commission v Italy*, para 46; *ZZ v Secretary of State of the Home Department*, para 45.

Varying Degree of Restrictiveness

Although data localisation measures share a common denominator in the objective to forcefully keep data within a certain jurisdiction, their intrusiveness can vary. The implementation of such requirements could be merely a requirement to store a copy of the relevant data somewhere within the national territory, which may seem as a relatively light restriction on cross-border trade. In reality, firms rarely have the financial overhead to store business data on multiple locations, why even a storage requirement bars firms and governments from using suppliers from other EU Member States.

In more restrictive cases, individual EU Member States impose outright prohibitions on processing or transferring the data overseas. This forces the firm to use, process and analyse their data inside the national territory. Such measures could make it de jure and de facto impossible to use foreign suppliers, and even prohibit copies of certain data to be transferred cross-border – for example to a wholly-owned subsidiary or offices in another EU Member State.

One special form of processing and transfer restrictions are laws that stipulate restrictive conditions for transferring data overseas. Under such regime, data cannot flow to another EU Member State unless the firm fulfils certain conditions. In most of such cases, there are multiple and overlapping conditions that must be fulfilled, such as security standards, government approval or strict requirements on consent.

Explicit Data Localising Measures

Our survey has identified 22 regulatory measures imposed by EU governments which apply to intra-EU transfer of data:[17]

- The most common requirements relate to accounting information and financial statements. Such requirements can be quite extensive as in the case of Germany – where all invoices, books and records, accounting documents and commercial letters are required to be stored in the country, albeit subject to certain exceptions; another example is the Danish Book Keeping Act, which requires that companies' financial records must be stored in Denmark, or in one of the Nordic countries. In case the records are stored on a server physically placed outside Denmark or on the cloud, a complete copy must be kept inside Denmark. Similar requirements are found in Belgium, Finland, Sweden and the UK.

- The second most common area concerns gambling. In three European countries (Bulgaria, Poland and Romania), data localisation requirements are imposed on winnings and user transactions. In Bulgaria for example, an applicant for a gaming license must assure that all data related to operations in Bulgaria is retained on a server located within the country, whereas the communication equipment and the central computer system may be located within the European Economic Area (EEA) or Switzerland.

- General stipulations on publicly held records are imposed in Denmark, the Netherlands, Sweden and the UK. This is often limited to a specific set of data, as in the case of Denmark, where only financial records for governmental institutions must be stored within the country; in the Netherlands, the requirements apply to all public records; in the UK, overseas processing of healthcare data held by the National Health Services (NHS) could be restricted by its information governance rules.

- In France, the decree amending the Code of Electronic Communications includes a 'territorial restriction' requiring that the systems for intercepting of electronic communications must be installed and all data must be processed in France. Also, in some Member States, there

[17] ECIPE Digital Trade Estimates, 2016.

are data retention requirements that are designed as data localisation measures. Such requirements persist despite the invalidation by the European Court of Justice (ECJ) of the Directive on data retention. The Greek Law No. 397/211 goes further in the implementation of the Data Retention Directive by requiring that retained data on traffic and location stays within the Hellenic territory; Germany has recently passed a law with similar effect.

- The financial supervision authority in Luxembourg requires client data to be stored and processed locally; Sweden (with possibly other Member States) requires immediate access to data held by a financial institution, which is interpreted as authorities must have immediate physical access at the location, and therefore require that certain data remain within the territory.

Table 1: List of identified local storage and processing measures implemented within EU

Belgium	Article 233 of the Companies Code requires that the Company register of shareholders and register of bonds must be kept at the registered office of the company. Since 2005, it is possible to keep the registers in electronic format as long as they are accessible at the registered office of the company.
Belgium	With respect to VAT, invoices received and copies of invoices issued by the taxpayer must be stored in Belgium or in another EU member state under certain conditions. Invoices must be stored either in electronic or paper format (Article 60, § 3 of the VAT Code).
Belgium	With respect to income tax, except in case of exception granted by the administration, the books and documents must be kept at the disposal of the tax administration in the office, agency, branch or other professional or private premises of the taxpayer where they have been kept, prepared or sent.
Bulgaria	In Bulgaria, an applicant for a gaming license must assure that all data related to operations in Bulgaria is stored on a server located in the territory of Bulgaria. Moreover, the applicant has to assure that the communication equipment and the central computer system of the organizer are located within the EEA or in Switzerland.
Denmark	The basis of the Bookkeeping Act (section 12) in Denmark is that financial records must be stored in Denmark or in the Nordic countries. This applies to both physical appendixes and digital data. Hence, if financial records are stored on a server physically placed outside Denmark a complete copy must be kept in Denmark.
Denmark	The basis for the Audit Act (section 45) in Denmark is that financial records for governmental institutions must be stored in Denmark. This applies to both physical appendixes and digital data. This regulation means that financial records may be stored on a server abroad provided that an exact copy of the records is made on a monthly basis at a minimum. Such copy must be placed on a server in Denmark or in paper.
Finland	The Accounting Act requires that a copy of the accounting records in kept within Finland. Alternatively, the records can be stored in another EU country if a real time connection to the data is guaranteed.
France	Through a decree amending the Code of Electronic Communications, France has included a "territorial" restriction" requiring that the systems for interception of electronic communications must be established in France.
Germany	The Act on Value Added Tax states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electronic storage, they may be stored within the territory of the EU if full online access and the possibility of download are guaranteed. In this case, the entity is obliged to notify the competent tax authority in writing of the location of the electronically stored invoices, and the tax authority may access and download the data.
Germany	Under the Tax Code, all persons and companies liable to pay taxes that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.

Germany	According to the German Commercial Code, accounting documents and commercial letters must be stored in Germany.
Germany	In 2010, the German Constitutional Court found the implementation of the Directive on Data retention was unconstitutional. Yet, in October 2015, a new data retention law has passed, which will enter into force in 2017. The law provides that telecommunication providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either four or 10 weeks. The data is to be stored in servers located within Germany (§113b).
Greece	In Greece, the Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later annulled by the European Court of Justice) by requiring that retained data on 'traffic and localisation' stay 'within the premises of the Hellenic territory.'
Luxembourg	According to the Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.
Netherlands	Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records.
Poland	According to the Polish Gambling Act, any entity organizing gambling activities is obliged to archive in real time all data exchanged between such entity and the users in an archive device located in Poland.
Romania	In Romania, the game server must store all data related to the provision of remote gambling services, including records and identification of the players, the stakes placed and the winnings paid out. Information must be stored using data storage equipment (mirror server) situated on Romanian territory.
Sweden	In Sweden, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in Sweden for a period of seven years.
Sweden	In relation to specific government authorities, there are certain provisions which might require the data processed by the authority to be held within Sweden or within the authority. This might affect the supply of cloud computing to certain authorities.
Sweden	The Financial Services Authority require "immediate" access to data in its market supervision which, according to business, the supervisory body interprets as been given physical access to servers. Accordingly, Swedish financial services providers are de facto required to maintain all its records inside Swedish jurisdiction
United Kingdom	According to the Companies Act 2006, "if accounting records are kept at a place outside the United Kingdom, accounts and returns (..) must be sent to, and kept at, a place in the United Kingdom and must at all times be open to such inspection."
United Kingdom	In the United Kingdom, there are no legal prohibitions on exporting NHS patient data outside the country. However, the NHS and associated institutions are bound by strong legal, ethical and regulatory obligations of confidentiality. The location outside the UK of the data recipient is considered a risk factor by the NHS information governance rules and therefore might result in localisation of data.

Source: ECIPE Digital Trade Estimates, 2016.

Data localisation measures are not the only measures impacting the flow of data. There are several other measures which prevent data to flow freely, regardless of whether the data crosses or not borders. Several of these measures also apply within the European Union and they often refer to cloud computing applications or to data from the telecommunications sector. Most of these indirect measures are likely not actionable under the Digital Single Market strategy: They lack an explicitly geographical element that makes a distinction between domestic and other EU undertakings that apply in a horizontal manner to domestic and foreign companies alike.

Such indirect measures have not been included to the scenarios we analyse in this paper. For a comprehensive list of other restricting measures on the use of data that implicitly and indirectly lead to data being stored in a certain jurisdiction is listed in Annex II.

Fact box: A case study on the impact of accounting related data on SMEs

Small and Medium Sized Enterprises (SMEs) are more vulnerable to costs arising from domestic regulations, as they are less able to adjust their supply chains, human resources or to invest in alternative solutions. Given their smaller scale, they must also distribute fixed costs resulting from regulations over a smaller volume of sales compared to larger firms. This is why local storage requirements disproportionately affect SMEs, even for seemingly minor requirements, such as those related to accounting data.

The EU Single Market is still a patchwork of national accounting rules that particularly constrains SMEs. Given certain conditions, EU firms may be required to file tax declarations in another EU Member State when they have customers there. If that country also requires accounting records to be on local servers, SMEs would be required to hire a local external accountant to store a copy of its files – unless the SME already has a physical establishment there. While this requirement would have trivial costs for multinationals, it could become a decisive factor for a small company.

In addition, the scope of the data localisation measures on local storage differ from country to country, making it even more costly and complex to comply with national regulations. For example, in Belgium, firms are required to retain their invoices in Belgium (Article 60 of the VAT Code), while books and other documents related to income declarations must be kept at the disposal of the tax administration in the office, agency, branch or other professional or private premises of the taxpayer where they have been kept, prepared or sent (Article 315 of the Income Tax Code) under certain conditions.[18] In Germany, the Act on Value Added Tax states that company invoices must be stored within the country in some cases; the German Tax Code also requires all firms liable to pay local taxes to keep their books and records within the country; the Commercial Code put similar requirements on accounting documents and commercial letters.

Considering that SMEs account for nearly 60% of European GDP and 65% of European employment, streamlining data storage requirements would have a significant impact given the great number of SMEs – and in turn, on the efficiency of intra-EU goods and services provision.

3. TWO SCENARIOS: LIBERALISATION AND RATCHET

This study builds on two scenarios. The first scenario – denoted as the liberalisation scenario – assumes that the regulatory data localising measures outlined in the previous section are liberalised. Specifically, the economic impact of liberalising the existing directly and explicitly data localising measures is estimated on the basis of two different methodological approaches.

[18] See De Brauw, Blackstone, Westbroek, 2013.

Second, the study looks at a scenario where cross-border data flows within the EU would be restricted by all EU Member States, imposing data localisation requirement across the EU thereby effectively ceasing the cross-border use of online applications and data. The negative economic loss from data localisation determines the value of the preventive measure of banning such practices internally within the Single Market like a ratchet clause – hence, the scenario is denoted the ratchet scenario. This scenario builds on previous work of the authors,[19] but is limited to the localisation barriers alone without other administrative requirements (e.g. compliance costs for data privacy regulations), which were within the scope of the previous studies.

A Liberalisation Scenario

The extent of unnecessary economic losses caused by direct and explicit localisation measures is determined by a series of factors. Firstly, firms and public services that were previously required to store and process data within a certain Member State would have access to lower prices for data services "produced" in other EU countries. The economic savings for these firms or public services are the result of static effects from lower costs and a more efficient allocation of resources across the economy, which would improve the individual firms' productivity, and in turn boost competitiveness, lower prices, and increase domestic and foreign demand.

Two alternative approaches are deployed for this scenario:

- The first approach assumes a reduction of prices as the lower price available in the other EU Member States becomes available. The cost changes are implemented as ad valorem equivalents (AVEs), while assuming that the bias for domestic suppliers vis-a-vis foreign suppliers is assumed to be unchanged. In other words, the buyers' preference for local suppliers (due to proximity, established commercial relations, currency risks, language barriers) remains. This approach approximates the trade effects under a fully price-transparent "industrial" DSM.

- The second approach considers a productivity improvement in the economies where the use of data storage or processing from another EU Member State was previously restricted. Such costs and their effect on total factor productivity (TFP) can be measured in real-life surveys and indirectly through econometric techniques. These costs are passed on downstream to customers – who may be manufacturers, exporters, a public agency, or private households – and further reduce productivity. The effect is factored by severity of the existing localisation measure, depending on whether the measure imposed is a storage or processing requirement, and the type of data that is affected. Similar to the first scenario, the sectoral scope of the current localisation measures is taken into account.

Both approaches to the liberalisation scenario compare the cost of using data, i.e. processing, managing and administrating data, as well as building or leasing data centres. The cost difference storing data can be considerable amongst the EU Member States – with a variance up to 120%, more than twice the cost in the most expensive Member State compared to the cheapest. It should be noted, however, that the assessment of prices of data storage and processing is complex and difficult to generalise: the actual costs vary depending on actual set-up and scale; unlike generalised commodities like oil, the cost of data storage or processing varies highly within an economy. The prices are approximated through the general cost levels of inputs going into operating services – including energy, land prices, bandwidth, ease of doing business.[20] Risk and policy factors are also accounted for, but given considerably lower weights.[21]

[19] See International Economics, 2015; ECIPE, 2014.
[20] Greenberg, Hamilton, Maltz, Patel, The Cost of a Cloud: Research Problems in Data Center Networks, Microsoft Research, accessed at: http://research.microsoft.com/en-us/um/people/dmaltz/papers/DC-Costs-CCR-editorial.pdf.
[21] Cushman & Wakefield, Data Centre Risk Index 2013.

Both approaches also look to a number of important dynamic effects from the trickle down of price changes throughout the economy: data storage accounts for up to 1.9% of the inputs used in producing services –[22] with ICT consulting activities, software and connectivity provision, the importance of data-related activities increases up to 31% of services inputs.[23] Moreover, the impact of price changes affects also the prices outside the ICT sector. In both approaches, the impact also depends on whether the restriction relates to mere local storage requirement or local processing.

A Ratchet Scenario

The "ratchet" effect scenario estimates the impact of economy-wide data localisation requirements imposed by all 28 EU Member States. This is the overall nominal value of the economic damage that a data localisation discipline could prevent.

In this scenario, it is assumed that firms can no longer use their IT infrastructure, application suppliers or data centres located in another EU Member State to process the data collected in a certain Member State. Therefore, data centres must be set up, or outsourced to a local service provider in each of the Member States by both foreign and domestic enterprises. This increased cost is passed on to the customers, who may be manufacturers, exporters or final consumers. This leads to productivity losses for various sectors and downstream industries.

As often with all type of scenario analysis, this "worst case" scenario may not be realised. However, determining which EU Member State, or which sector that may be subjected to data localisation in near future would be purely speculative. Therefore, it is preferable to have a clear scenario based on maximum potential economic damage, prevented by a data localisation ban.

Similar to the TFP approach under the liberalisation scenario, the ratchet scenario builds on the observed relations between price increases of inputs and TFP at industry level for domestic firms, based on previous work on data localisation by the authors. Unlike the previous studies, it builds on actual cost levels as observed in the EU and it only includes the productivity loss element, whereas previous studies built on a conceptual model that included compliance costs for privacy regulations (GDPR) and miscellaneous dynamic effects from investments and R&D.

4. RESULTS

Effects from the Liberalisation Scenario

The results show that the benefits resulting from an elimination of current data localisation measures are comparatively low, given that most of the measures are limited in scope and restrictiveness. Yet, such gains have a certain weight in the current economic climate where the level of economic growth in the EU was 2% in 2015 and projected to decline to 1.8% in 2016.[24] Under the liberalisation scenario, i.e. the abolition of currently imposed direct data localisation measures where such regulations were identified, following GDP gains are generated:

[22] US Bureau of Economic Analysis, Input and Output Accounts Data, 2007.
[23] ibid.
[24] IMF, World Economic Outlook, 2015.

Table 2: GDP gains from liberalising current data localisation measures

Belgium	0.06~0.18%
Denmark	0.00~0.02%
Finland	0.01~0.06%
Germany	0.05~0.07%
Greece	0.01~0.09%
Luxembourg	0.02~1.10%
The Netherlands	0.03~0.04%
Sweden	0.03~0.05%
The UK	0.05~0.05%

Source: Own calculations based on GTAP8.

The two alternate approaches used under this scenario create a span in GDP gains above, where notably Luxembourg is a potential outlier given the size of its financial services sector relative to its economy.

Furthermore, one of the approaches (the so-called AVE based approach) also assess the impact from lower prices for data storage and processing (based on differences against lowest prices registered in the EU), while buyers' preferences for sourcing such services locally is left unchanged. This simulation is a close approximation of increased competitive pressure under a fully price-transparent "industrial" DSM, generating GDP gains up to 0.06%. In absolute numbers, the overall EU-wide weighted impact is up to 8 billion euros yearly based on current EU GDP. The true cost of today's restrictions is likely to be underestimated given that this scenario does not take into account the regulations that are implicitly or indirectly localising data.

It is worth noting that the impact of these price adjustments would not lead to a large-scale outsourcing of data hosting and processing services to other EU Member States. Imports of communication services by German customers from other EU Member States would increase within a range of 2~8% above today's levels; or 2~14% in the case of France. In all other cases, the import increase on communication services are limited to between zero and 3%.

Effects from the Ratchet Scenario

The lion share of the economic gains from a ban on data localisation are derived from the ratchet effect – i.e. from preventing EU Member States from imposing economically harmful data localisation measures in the future. In this scenario, it is assumed that each EU Member State imposes a regulatory requirement to store and process data locally, applied erga omnes – including other EU Member States. The GDP impact falls within a relatively narrow range of -0.27% (in Romania) to -0.61% (in Luxembourg) . The variance largely reflects the structural sectoral composition (i.e. the prominence of data-intensive sectors) or the service dependency of the economy. The overall EU-wide weighted impact is approximately 0.4% or 52 billion euros annually.

The output losses are notable across all services sectors and Member States. However, they are particularly pronounced in the communication sector. In other words – data localisation measures are unlikely to support domestic ICT and telecom sectors through diverting local business and job opportunities to local market actors, displacing their EU or foreign competitors. The productivity losses in the economy generate much bigger losses throughout the economy, i.e. the economic loss resulting from forgone economic activities considerably exceed the marginal economic gains from protecting domestic data and communication sectors.

Table 3: GDP losses of EU Member States from imposing data localisation measures

	GDP loss	Output loss in communication/ ICT
Austria	-0.37%	-1.67%
Belgium	-0.40%	-1.39%
Bulgaria	-0.46%	-0.96%
Croatia	-0.31%	-1.67%
Cyprus	-0.36%	-1.66%
Czech Republic	-0.46%	-0.89%
Denmark	-0.36%	-1.69%
Estonia	-0.48%	-1.01%
Finland	-0.41%	-0.61%
France	-0.44%	-0.74%
Germany	-0.33%	-0.79%
Greece	-0.31%	-0.81%
Hungary	-0.45%	-0.99%
Ireland	-0.40%	-1.27%
Italy	-0.42%	-0.89%
Latvia	-0.31%	-0.81%
Lithuania	-0.32%	-0.93%
Luxembourg	-0.61%	-3.46%
Malta	-0.28%	-3.14%
Netherlands	-0.40%	-1.23%
Poland	-0.39%	-0.54%
Portugal	-0.42%	-1.03%
Romania	-0.27%	n/a
Slovakia	-0.47%	-0.67%
Slovenia	-0.40%	-1.29%
Spain	-0.36%	-0.66%
Sweden	-0.43%	-1.05%
United Kingdom	-0.30%	-0.67%

Source: Own calculations based on GTAP8.

5. CONCLUSIONS

Data localisation policies come at severe costs, often being counterproductive to the alleged policy objectives. In the short-run, forced data localisation causes losses of firm-level productivity, higher prices, decreases in competitiveness, fewer jobs and lower economic activity. In the long-run, data localisation makes a country less attractive to foreign investment, giving arise to local oligopolies, encourages consumer lock-in effects that deprives an economy of its innovative potential.

The effects of liberalising existing measures are at 8 billion euros per year, on par with the effects of recent free trade agreements that the EU has concluded, including the EU-Korea FTA and Comprehensive and Economic Trade Agreement (CETA) with Canada.[25] However, the greatest economic impact is from preventing the Member States from being drawn into the global policy inclination towards "data nationalism". The effects of such ratchet – equivalent to 0.37% of EU GDP – is worth six times more than the liberalisation of existing Member State measures.

[25] The EU-Korea FTA was expected to generate 0.03% to 0.08% of EU GDP (see Francois, Economic Impact of a Potential Free Trade Agreement (FTA) Between the European Union and South Korea, Copenhagen Economics, 2007; also Decreux, Milner, Peridy, The Economic Impact of the Free Trade Agreement (FTA) between the European Union and Korea, CEPII/ATLASS, 2010); EU-Canada FTA (CETA) is assumed by the contracting parties to generate 0.08% of EU GDP (European Commission, the Government of Canada, Canada-EU Joint Study, Assessing the Costs and Benefits of a Closer EU-Canada Economic Partnership, 2008).

In the long term, the political imperative goes beyond just the digital economy: as goods, services and investments rely increasingly on effective, real-time sharing of data and use of applications across the Single Market, Europe would be eroding its internal market and effectively roll-back on existing Single Market commitments. If the use of data-related inputs to the industry are doubled in the near future, up to 0.8% of EU GDP could be at stake.

As convincing as this economic threat is, more is at stake: Even in the immediate short term, a ban on data localisation is a powerful political message that the Single Market is open for business. This is how this policy initiative finds its most convincing rationale – by delivering an assurance of legal certainty for EU business going forward, and that the Member States will withstand the global trend towards localised data. A ban on internal data localisation in the EU draws the line on future attempts to roll back on the commitment to keep the Single Market seamless across Europe. This argument is particularly pertinent as the EU seeks to convince the market and turn the tide on the digital investments, and both inward and domestic investments into Europe's digital economy are withheld or diverted to other regions.

Ultimately, whether the EU will succeed in creating a DSM that benefits the consumers and the industry depends on whether the EU will withstand the trend towards data localisation. However, the current window of opportunity to act – while the internal Member States' measures remain relatively few – is not likely to last for long.

ANNEX I: METHOOLOGICAL NOTES

The model applied in this study is GTAP 8, a computable general equilibrium (CGE) model.[26] The model is frequently applied by academia and international institutions including the European Commission's DG Trade to estimate the impact of regulatory changes on a broad set of macro-economic and sector-specific economic variables.[27] The model setting accounts for inter-sectoral linkages between 129 regions while capturing inter-regional trade flows of 57 commodities. The framework thus allows for a general equilibrium analysis of the economic effects (e.g. GDP effects and changes in trade flows) resulting from the regulation of cross-border data flows in the EU28. In this model, regional production is characterized by constant returns to scale and perfect competition. Private demand is represented by non-homothetic consumer demands. The structure of foreign trade is based on the so-called Armington assumption, which implies imperfect substitutability between domestic and foreign goods. The dataset includes national input-output data as well as trade, tariffs and demand structures. The model's base data are primarily benchmarked to 2007.

Like any applied economic model, this model is based on a number of assumptions. In order to account for recent changes in regional macroeconomic variables, the dataset on the global economy is extrapolated to 2016. The exogenous variables used for the extrapolation are macroeconomic variables, i.e. the size of GDP, total population, labour force, total factor productivity and capital endowment as provided by the well-recognised database of the French research centre in international economics (CEPII).[28] We apply the estimates of these macroeconomic data projections in order to calculate the 'best estimate' of the global economy in 2016. Preferences and production structures as described by the model's structural parameters have been left unmodified.

The model applied in this study is comparative static. It does not account for endogenous productivity growth and may thus under-predict welfare effects, growth in economic activity and increases in trade flows that result from data regulation-induced sectoral productivity changes. Our estimates on data regulation-induced changes in productivity are incorporated by the application of output augmenting technical changes on a sector-by-sector-basis. For the ratchet scenarios, the simulation of data regulation-induced price effects is based on an import-augmenting tech change variable, which is also applied on a sector-by sector basis (ad valorem equivalents, AVEs). The latter variable accounts for efficiency improvements or efficiency deteriorations in the facilitation of trade between two regions or countries respectively.

The methodology for estimating TFP losses is extensively described in previous work of the authors.[29]

[26] Hertel, Tsiga,1997.
[27] Francois, 2007, 2013.
[28] Foure, Benassy-Quere, Fontagne, 2010.
[29] see van der Marel et al., 2015 and Bauer et al., 2014.

ANNEX II: OTHER RESTRICTING MEASURES THAT IMPLICITLY AND INDIRECTLY COULD LEAD TO DATA LOCALISATION

In addition to the internal data localisation measures present above, there are other measures in the EU which are not directly imposing localisation of data, but could lead to similar results. Typical examples of such measures are EU-wide rules that restrict storage of banking information on cloud services. Such requirements do not explicitly ban moving data to another Member State per se, but cloud solutions are likely to be hosted in another EU Member State or elsewhere. Similarly, the prerogative of the Member States to specify additional conditions beyond the Data Privacy Directive (e.g. for sharing of personal information for marketing purposes) does not necessarily single out overseas data processors, but it is very likely to do so given that authorities would have few legal grounds to exercise their jurisdiction even if the processor is based in another Member State.

A special example concerns data retention. Under the Data Retention Directive,[30] which was recently declared invalid by the CJEU,[31] EU telecom operators were required to retain traffic and location data for a period between six months and two years and to make them available to law enforcement authorities. In some Member State jurisdictions, the revocation of the directive is yet to be implemented, and therefore it remains still in force. Even in the cases where it is not required to store the retained data within the country, data retention requirements induce a localising effect as operators must invest in considerable storage capacities in close proximity to a physical infrastructure that is present in the country – making it less likely to invest in additional storage and processing capacities overseas.

It is worth noting that many of the measures in this category may not be actionable through a data localisation ban, as they are not explicitly localising and de jure non-discriminatory between domestic and foreign companies. Other measures clearly fall within the scope of the national security exception. Reforming the rules in certain sectors, e.g. banking, entails additional political processes and mandates beyond the scope of DSM. Meanwhile, some of the implicit and indirect requirements here are transitory – for instance, aforementioned Directives on Data Protection and Data Retention have been reformed and revoked, respectively.

[30] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[31] *Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources*, C–293/12.

Table A-1: List of other identified measures restricting the flow of data implicitly or indirectly within the EU

EU-Wide	Several norms regulating the outsourcing of information processing apply specifically to the operations of the banking sector in each of the Member States, and impose restrictions on the usage of cloud storage in the banking sector, whether the data is stored domestically or overseas. These norms often result from transposition of European Directives and guidelines, e.g. the Commission Directive 2006/73/EC of 10 August 2006 regarding operating conditions for investment firms and defined terms for the purposes of that Directive and the guidelines on outsourcing published by the Committee of European Banking Supervisors.
EU-Wide	According to the Directive 95/46/EC, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies, and Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing subject to the provisions allowing a data subject to object to the processing of data regarding them, at no cost and without having to state his reasons.
Austria	For all EU countries, consent for collection of data is required. However, in the case of Austria, there is a stricter requirement for a data subject's consent to be valid, e.g. - the data subject must be provided with all relevant information about the data to be processed, the purpose of the respective data processing and any potential data recipients; - the consent must be given without any restraints (hence, the Austrian courts are frequently reluctant to accept the validity of employee consent); and - the data subject has to receive explicit information about his right to revoke his consent at any time, without giving reason for such revocation.
Cyprus	Under the Directive on Data Retention, operators were required to retain certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism. On 8 April 2014, the Court of Justice of the European Union declared the Directive invalid. However, not all national laws which implemented the Directive have been overturned. The Cyprus Supreme Court decided on 1 February 2011 that some of the provisions of Law 183 (I)/2007 implementing of the EU Data Retention Directive are unlawful. However, most of the provisions of the Directive still apply.
Denmark	Since 2011, the Danish Data Protection authority has ruled in several cases against processing of local authorities' data in third countries (non-EU) without using standard contractual clauses. This is the result of a strict interpretation of the European Directive 95/46/EC. Therefore, services such as Dropbox, Google Apps and Microsoft's Office 365 cannot be used by local authorities unless they have signed an agreement with the processor based on standard contractual clauses.
Denmark	The Danish law on data retention is still into force after the ECJ ruled the Data Retention Directive invalid. However, it now does not affect session logging requirements.
Denmark	In 2011, the Danish Data Protection Agency denied the city of Odense permission to transfer "data concerning health, serious social problems, and other purely private matters" to Google Apps, citing security concerns. In its opinion, the Agency specified that the reason behind the decision lies on the impossibility to assess whether "all of Google Inc.'s data centres in Europe are located within the EU/EEA".

Finland	In Finland, data retention laws are still in force. However, following the ECJ ruling invalidating the Data Retention Directive, the scope and the application of the Finnish Information Society Code has been limited. For instance, it does not include web browsing data. Smaller operators are exempt from retaining their data. The data retention period goes from six months to 12 months, according to the category of the data.
France	France has not overturned the data retention law (French Decree No 2006-358) and, therefore, telecommunication operators, both internet and phone operators, must retain their data for one year.
France	In December 2013, France adopted the Military Programming Law permitting both the security forces and intelligence services from various ministries (defense, interior, economy, and budget) to see "electronic and digital communications" in "real time." Under the law, agencies have until 48 hours after surveillance has begun to seek approval from the National Commission for the Control of Security Intercepts (CNCIS) president and can continue while awaiting his/her decision. The law came into force in January 2015.
France	The French Blocking Statute (Law No. 80-538) prohibits any French party from disclosing commercial information whether originating from France or elsewhere in foreign litigation, absent a French court order, if such information might impact the security of the country. Therefore, such data cannot be sent (also electronically) to other countries.
France	Article 65 of the Defence Decree provides that documents marked as 'Special France' which the issuing authority regards that they should be disclosed only to French citizens and under no circumstance to foreigners.
France	Hosting providers of health data have to go through an accreditation procedure pursuant to Article L-111-8 of the French Public Health Code. Once accredited, the hosting provider and the health data manager should enter into an agreement organizing the terms of access to and storage conditions of such health data, in order to ensure their sustainability and confidentiality.
Germany	For all EU countries, consent for collection of data is required. In Germany, consent must be based on the data subject's free decision and should be in writing, unless special circumstances dictate otherwise. Strict rules have been established concerning the purposes of selling addresses and using contact details for marketing which will be permitted only if the individual has expressly consented to such use.
Germany	In general, the storage and processing of public registers / records with sensitive data of citizens (such as records of the tax authority or criminal records or registers of births, marriages and deaths or weapon registers or registers of data of social security institutions) may not be outsourced outside the public entity. Moreover, restrictions on cloud computing may arise from the exclusive access of civil servants to the exercise of sovereign powers, which is granted by the German Constitution (Art. 33(4)). The requirements vary between different States in Germany. For example, in Brandenburg the authorities which store a register of the residency of Brandenburg's citizens are only allowed to use private Cloud Computing services which are located in Brandenburg (Sec. 35 BbgMeldeG). In August 2015, Germany issued nationwide guidelines that prohibit government agencies from using clouds to store sensitive data if the cloud company processes data outside the Germany. Cloud providers could qualify for the "German cloud" certification if their servers and company headquarters are located in Germany. However, the proposal was later withdrawn.

Germany	The use of Cloud Computing services may – depending on the information stored and the purpose of storing these information – constitute a disclosure of confidential information in violence of professional secrecy in the meaning of Sec. 203 StGB (German Criminal Code). The professional secrecy includes personal data as well as all facts, which are obtained for professional reasons. Professionals that are subject to professional secrecy are especially, but not exclusively, lawyers and legal professionals, medical professions, social care, clerical professionals and civil servants. As an example, such legislation results in public hospitals requiring prior consent of the subject or prior anonymisation of the patient data in order to use IT services external to the hospital.
Germany	In general, the collection, use and processing of social data shall be entrusted to public servants who owe their services and loyalty to the state. The use of cloud solutions from private entities is subject to certain restrictions. It must ensure the absence of disturbances during the operations, lead to significant cost savings and the major part of the database has to remain with the respective public authority.
Germany	In certain German states, public and private hospitals can use external IT service vendors if they obtain prior consent from the data subject or if there is prior anonymisation of the patient data.
Germany	The use of Cloud Computing services may be subject to export control, if the respective data are technical data intended for the production or use of goods under export control according to the Foreign Trade and Payments Ordinance.
Germany	According to the German Banking Act, it must be ensured that the use of cloud services in the financial sector neither affects the regularity of services nor the business organisation.
Greece	In Greece, the government is considering the possibility of invalidating the national law on data retention (National law 3917/2011), but so far the law is still in force. Data must be retained for a period of 12 months and it needs to be retained within the Hellenic territory.
Hungary	The Hungarian Act on Electronic Communications requires 12 months' retention for all data which are not calls. Legislation is still in force despite the ECJ ruling.
Ireland	In Ireland, the Communications (Retention of Data) Act 2011 requiring 13 to 25 months data retention is still in force notwithstanding the ECJ ruling.
Italy	Article 39 of the Presidential Decree no. 633 of 1972 states that accounting data for VAT declarations might be kept in a foreign country only if some kind of convention has been concluded between Italy and the receiving country governing the exchange of information in the field of direct taxation.
Italy	In Italy, the Directive on Data Retention has been implemented through an amendment to the Privacy Code effective as of August 2009 and still applying today. Under the Privacy Code, providers of a public communications network or a publicly available electronic communications service must retain "telephone traffic data" and "electronic communications traffic data" for 24 months or 12 months, respectively, for law enforcement purposes. A 30 day retention period applies in case of data related to unsuccessful calls processed on a provisional basis.
Latvia	In Latvia, a data retention period of 18 months is still in force despite the ECJ ruling.
Poland	In Poland, the national law on data retention is still in force despite the ECJ ruling invalidating the Data Retention Directive. The data retention period is 24 months.
Poland	Poland required e-commerce entities to store customer details in Poland. After intervention by the European Commission, Poland was forced to lift the requirement and it is now sufficient that the servers are located in one of the EU countries.

Poland	According to the Polish Gambling Act, the equipment (servers) for processing and storing information and data regarding the bets and their participants must be installed and kept on the territory of a member state of the EU or EFTA.
Portugal	The law on data retention is still in force in Portugal. The retention period is 12 months.
Romania	In Romania, any transfer of personal data to any state requires prior notification to the National Supervisory Authority for Personal Data Processing (NSAPDP). Moreover, any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.
Slovenia	The Privacy Act contains a specific requirement for the so-called "traceability of processing of personal data". It requires that the data controller and data processor enable subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and by whom (Art. 24).
Spain	In Spain, Law 25/2007 relative to retention of data relating to electronic communications networks and public communication, effective from November 2007 is still in place. Such law is only applicable to electronic communications operators and provides for a retention period in respect of traffic data of 12 months from the date on which the communication occurred.
Sweden	espite the ECJ ruling, the law implementing a data retention period of 12 months is still in force in Sweden. After the ruling, there have been some reported cases of companies that did not incur in any enforcement measure for not having stored their data.
UK	In November 2015, the Secretary of State for the Home Department presented the 'Draft Investigatory Powers Bill' to the Parliament. Clause 71 of the Bill requires web and phone companies to store records of websites visited by every citizen for 12 months for access by police, security services and other public bodies. In June 2016, the Investigatory Powers Bill has passed the House of Lords on 16 November 2016 and has to receive Royal Assent before it can be brought into force.

Source: ECIPE Digital Trade Estimates, 2016.

w

REFERENCES

Andriamananjara, Dean, Feinberg, Ferrantino, Ludema, Tsigas, The Effects of Non-Tariff Measures on Prices, Trade, and Welfare: CGE Implementation of Policy-Based Price Comparisons, USITC Economics Working Paper No. 2004-04-A.

A. Chander, U. P. Lê, Breaking the Web: Data Localization vs. the Global Internet, Working Paper 2014-1, California International Law Center, 12.03.2014, accessed at: http://ssrn.com/abstract=2407858, 20.03.2014.

Bauer, Lee-Makiyama, van der Marel, A Methodology to Estimate the Costs of Data Regulation", International Economics, 2015.

Bauer, Lee-Makiyama, van der Marel, The Cost of Data Localisation, ECIPE, 2014.

Bauer, Lee-Makiyama, van der Marel, Verschelde, A Methodology to Estimate the Cost of Data Regulations, ECIPE, 2014.

Bauer, Lee-Makiyama, Erixon, The Economic Importance of Getting Data Protection Right, US Chamber of Commerce, 2013.

Bauer, Lee-Makiyama, van der Marel, Verschelde, Data Localisation in Russia: A Self-Imposed Sanction, ECIPE, 2014.

Borggren, New Research: Conflicting Company Data Rules Inhibit Intra-EU Business, Project Disco, 2016, accessed at: http://www.project-disco.org/information-flow/022316-new-research-conflicting-european-accounting-rules-inhibit-intra-eu-business/#.V0s1cVcTWc9.

Cushman & Wakefield, Data Centre Risk Index 2013, accessed at: http://www.cushman-wakefield.pt/en-gb/research-and-insight/2013/data-centre-risk-index-2013.

De Brauw, Blackstone, Westbroek , EU Country Guide Data Location & Access Restriction, 2013 accessed at: http://www.verwal.net/wp/wp-content/uploads/2014/03/EU-Country-Guide-Data-Location-and-Access-Restrictions.pdf.

ECIPE, Digital Trade Estimates, 2016.

European Commission, A Digital Single Market Strategy for Europe, SWD(2015) 100, 6 May 2015.

European Commission, the Governent of Canada, Canada-EU Joint Study, Assessing the Costs and Benefits of a Closer EU-Canada Economic Partnership, 2008.

Foure, Benassy-Quere, Fontagne, The world economy in 2050: a tentative picture, CEPII Working paper 2010-27, 2010.

Francois, Reducing Transatlantic Barriers to Trade and Investment - An Economic Assessment, Final Project Report Prepared under implementing Framework Contract TRADE10/A2/A16, 2013.

Francois, Economic Impact of a Potential Free Trade Agreement (FTA) Between the European Union and South Korea, Copenhagen Economics, 2007.

Greenberg, Hamilton, Maltz, Patel, The Cost of a Cloud: Research Problems in Data Center Networks, Microsoft Research, accessed at: http://research.microsoft.com/en-us/um/people/dmaltz/papers/DC-Costs-CCR-editorial.pdf.

Hertel, Tsiga, Structure of GTAP. In Global Trade Analysis : Modeling and Applications. Ed. Thomas W. Hertel, Purdue University. Cambridge University Press. 1997.

IMF, World Economic Outlook, 2015.

OECD, Inter-Country Input-Output (ICIO) Tables, 2011.

Rentzhog, No Transfer, No Production, National Board of Trade of Sweden, 2015.

Rentzhog, Jonströmer, No Transfer, No Trade, National Board of Trade of Sweden, 2014.

US Bureau of Economic Analysis, Input and Output Accounts Data, 2007.

van der Marel, E., H. Lee-Makiyama, M. Bauer and B. Verschelde (2016) "A Methodology to Estimate the Costs of Data Regulation", International Economics, Vol. 146, Issue 2, pages 12-39.