RSC 2024/22
Robert Schuman Centre for Advanced Studies
Global Governance Society

WORKING PAPER

The Brussels effect in Africa: Is it beneficial for intra-regional trade in digital services?

Martina F. Ferracane, Simón González Ugarte, and Erik van der Marel

European University Institute
Robert Schuman Centre for Advanced Studies
Global Governance Society

The Brussels effect in Africa: Is it beneficial for intra-regional trade in digital services?

Martina F. Ferracane, Simón González Ugarte, Erik van der Marel

RSC 2024/22

ISSN 1028-3625

Published in July 2024 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy

With the support of the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Robert Schumann Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS) was created in 1992 and is currently directed by Professor Erik Jones, and it aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics. The RSCAS is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The Global Governance Programme

The Global Governance Programme is one of the flagship programmes of the Robert Schuman Centre. It is a community of outstanding professors and scholars, that produces high quality research and engages with the world of practice through policy dialogue. Established and early-career scholars work on issues of global governance within and beyond academia, focusing on four broad and interdisciplinary areas: Global Economics, Europe in the World, Cultural Pluralism and Global Citizenship. The Programme also aims to contribute to the fostering of present and future generations of policy and decision makers through its executive training programme: the Academy of Global Governance, where theory and 'real world' experience meet and where leading academics, top-level officials, heads of international organisations and senior executives discuss on topical issues relating to global governance.

For more information: http://globalgovernanceprogramme.eui.eu

Abstract

African countries are increasingly regulating personal data. The Brussels effect is strong in the region, with most African countries having adopted policies on personal data transfers and domestic data protection influenced by the European Union's General Data Protection Regulation (GDPR). The EU model is characterised by a comprehensive data protection regime and conditions applied to transfers across borders. In addition, several African economies have implemented stricter policies on data transfers, following the control model traditionally pursued in China. Previous research indicates that policies that restrict the transfer of data across borders are linked to reduced levels of trade in digital services, while a strong data protection regime supports trade in digital services by increasing consumer trust. However, there are no empirical studies with a specific regional focus on Africa. We use information on regulatory regimes in 54 African countries to estimate with a gravity model the impact of data policies on trade in services. Our analysis shows that the Brussels effect does not appear to be beneficial in promoting intra-regional trade as both the conditions applied to transfers across borders and the presence of ambitious data protection regimes domestically are associated with lower intra-regional trade in digital services, although the results differ by income level. We estimate that a regional commitment to open data transfers within the region could lead to an increase in intra-regional trade in digital services of up to 11%, amounting to 135 million USD.

Keywords

Cross-border data transfers; data protection; digital services; digital trade; regional integration.

Acknowledgments

This paper builds on research supported by the African Economic Research Consortium (AERC) as part of the Data Governance in Africa project - Grant No: RC23525.

Table of contents

1. Introduction

Cross-border data flows are a key priority for developing a digital single market in Africa, as evidenced by the discussions surrounding the Digital Trade Protocol of the African Continental Free Trade Area (AfCFTA).[1] The African Union (AU) Data Policy Framework[2] and the Digital Transformation Strategy of the AU Commission[3] underscore this common objective, advocating for the harmonisation of rules for cross-border data transfers among AU Member States.

While African countries discuss options to favour data transfers across borders and create a single market, restrictions on data flows keep rising in the region. Based on the data collected by the European University Institute (EUI) and the UN Economic Commission for Africa (UN-ECA) for a sample of 54 African countries[4] and published in the Digital Trade Integration (DTI) database,[5] 40 economies in the region restrict cross-border transfers of personal data by either requiring processing data locally or imposing conditions for data transfers. In this paper, we focus on policies applying to personal data, as they are driven by similar policy objectives and are expected to have a major impact on trade in services (World Bank, 2021). Yet, several additional policies that restrict data transfers in specific sectors are implemented in the region.[6]

These restrictions can create high trade costs for African businesses engaging in digital trade, which, in turn, are likely to impact the growth opportunities for the region. This is confirmed by a recent study performed by EUI and UN-ECA, which shows that cross-border data policies are associated with lower levels of trade in digital services (Ferracane and van der Marel, 2023). The study also finds that heterogeneity in the regulations on cross-border data flow also increases trade costs for digital trade.

This paper studies how different data models adopted in the region impact intra-regional trade in digital services. We do so by examining the regulatory model for the cross-border flow of personal data applied by each African country and estimating the extent to which sharing a similar data model is associated with greater or lower digital services trade between African countries. Regulatory frameworks for cross-border data transfers can broadly be categorised into three different models: open, conditional, or control model (Ferracane and van der Marel, 2021b). The open model is characterised by the absence of restrictions on cross-border data flows and the absence of a comprehensive framework for personal data protection that applies to domestic data processing. The presence of certain conditions for the transfer and processing of personal data characterises the conditional model, which is often influenced by the framework adopted by the European Union. The control model is defined by extensive restrictions applied to data transfers across borders, regardless of the presence of a data protection framework in the country.

We also study the additional effect of implementing a comprehensive data protection framework for processing personal data. On one hand, such a framework might increase the costs of doing business for firms, mainly in the form of compliance costs. On the other hand, it could also instil trust in the digital economy. In addition, as most countries have implemented a domestic regime for data protection influenced by the European Union model, the presence of a comprehensive data protection law could have a positive impact on trade by lowering regulatory heterogeneity.

1 The text of the Digital Trade Protocol of February 2024 has been leaked by Bilaterls.org and is available at the following link: https://www.bilaterals.org/IMG/pdf/afcfta_digital_trade_protocol_-_9_february_2024_draft.pdf

2 African Union (2022), Data Policy Framework, available at https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

3 African Union (2020), The Digital Transformation Strategy for Africa (2020-2030), available at https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

4 The countries included in the analysis are the following: Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cape Verde, Cameroon, Central African Republic, Chad, Comoros, Congo, Côte d'Ivoire, Djibouti, D.R Congo, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, São Tomé & Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia, and Zimbabwe.

5 Ferracane, M. F. (Ed.) (2022), "Digital Trade Integration Database", European University Institute *et al.*, available at https://dti.eui.eu/

6 For an overview of all policies restricting data transfers, see Ferracane and González Ugarte (forthcoming).

This paper is closely connected to an emerging series of empirical papers that study the impact of data-related restrictions on digital services trade (Ferracane and van der Marel, 2020, 2021a, 2024; López-González et al., 2020). It builds on this literature but with a specific focus on African countries. Using a gravity model, we estimate how sharing a data model and a comprehensive data protection law impacts intra-regional trade in digital services. The results of this analysis can eventually guide us in identifying the optimal regulatory data framework for the African continent to minimise trade costs in digital services.

The paper is organised as follows. The next section discusses further the related literature regarding data-related regulations and their impact on digital trade. Section 3 provides an overview of the three regulatory data models and shows which of the three models African countries currently apply for cross-border data transfers and which countries in the region implement a comprehensive data protection law. Section 4 describes our empirical approach to estimating the trade impact using the gravity model, whereas Section 5 provides the results. Finally, the last section concludes by providing policy insights based on our results.

2. Literature review

There is an emerging literature assessing empirically the extent to which data regulations potentially inhibit or stimulate trade and productivity. Ferracane and van der Marel (2021a) find that specific regulatory restrictions targeting the cross-border flow of data negatively impact trade in digital services across developed and developing countries. Similarly, for developed countries only, López-González et al. (2022) find that, although these measures raise demand for domestic ICT services, they also raise the costs of ICT inputs for other sectors, resulting in an overall negative impact on other sectors, which outweighs the positive impact on domestic data services.

The United States International Trade Commission (USITC) found that open data flows resulting from the implementation of the commitments in the US-Mexico-Canada USMCA would lead to a reduction in trade costs from these provisions, ranging between 1.1 and 1.4 percentage points, depending on the country (USITC, 2019). Ferracane et al. (2020) show that regulatory restrictions also inhibit local firms from reaping higher productivity gains.

Another strand of the literature assesses how the broader regulatory frameworks regarding cross-border flow and domestic data processing relate to trade in services. As noted in the World Development Report 2021 (World Bank, 2021), three global models regulating data are currently in place. The report and associated studies (Ferracane and van der Marel, 2021b, 2024) show that it matters to which regulatory model trading partners belong as different models have different impacts (positive or negative) on the ability of partner countries to trade services with each other. Using a gravity model with a sample of 143 economies, the authors find that a model based on open data transfers associated with a strong domestic data protection regime is the best suited to foster digital services trade. In contrast, restrictions on data transfers and the lack of domestic regulation on data protection can harm trade in digital services.

This paper also contributes to a broader strand of the literature covering research on the economics of privacy, including the economic value and consequences of protecting and disclosing personal data. Acquisti et al. (2016) provide a general overview of the theoretical and empirical research on the economics of privacy and show how the economic analysis of privacy has evolved and has become increasingly nuanced and complex with advancements in information technology. While comprehensive data protection regulations such as the European Union's General Data Protection Regulation (GDPR) can enhance online customers' trust (Zhang et al., 2020), they can also create significant compliance costs (Batikas et al., 2020; Chen et al., 2022).

Studies with a specific focus on intra-African digital trade are scarce. Some studies evaluate the benefits arising from higher integration of Africa in the global value chains (Fiorini et al., 2022), including through digitalisation (Cariolle and Piedade, 2023). One study shows that restrictions and regulatory heterogeneity on cross-border data flows are associated with lower levels of trade in digital services (Ferracane and van der Marel, 2023). However, the study looks at the bulk of policies and does not provide insights about the impact of specific types of policies on intra-regional trade.

Despite the rich policy debate on the need to harmonise data protection policies in the region, including in the context of the AfCFTA (Salami, 2022; Mozilla, 2022) and several authors inquiring about the necessity for the African region of data policies tailored to its needs and values (Makulilo, 2013; Mannion, 2020; Bryant, 2021), there are no empirical studies assessing the effect of data policies on intra-regional trade in Africa. This paper aims to fill this gap by combining varying strands of the literature regarding data restrictions, data protection, and data governance, with a unique focus on African countries.

3. Data policies in Africa

At the global level, three main regulatory models have emerged to regulate the cross-border transfers of personal data. The main features of these models are summarised in Table 1. The first model, which the United States traditionally advocates, is the open model. This model is characterised by the absence of restrictions on cross-border data flows. Countries following this model usually rely on a baseline set of privacy principles, leaving companies the flexibility to self-regulate on a voluntary basis. Under this model, firms usually remain accountable for how personal data is treated, including when it is transferred to a recipient in a third country. However, several countries following this model lack accountability for how personal data is treated after it crosses borders. This model also covers all those countries that simply still need to regulate the transfer of personal data. In general, countries that fall under this model consider data protection as a consumer right, and they usually lack a comprehensive framework for personal data protection that applies to domestic data processing.

The second model is the conditional model, characterised by the presence of certain conditions for the transfer of personal data across borders. Countries following this model take a comprehensive and fundamental rights approach to data protection with preventative regulation implementing certain conditions to be fulfilled ex-ante for the transfer of personal data across borders.[7] These conditions can be diverse, and include the consent of the data subject, the use of specific legal mechanisms such as binding corporate rules, the compliance with specific codes of conduct, or the requirement that the recipient countries have a regime for data protection considered ‘adequate’. In these countries, personal data protection is usually treated as a fundamental human right, and they usually implement a comprehensive regime for personal data protection at the domestic level. The European Union advocates this model in its GDPR[8], and before in its 1995 Directive for Data Protection, which established an international benchmark for data protection regulation. This model has exerted such an influence globally that scholars use the term “Brussels effect” to define this phenomenon (Bradford, 2020). As we will show below, Africa is no exception, with most of the countries in the region having adopted regulations heavily influenced by the GDPR.

7 In the case of the EU, which is the main actor embodying this model, the issue of privacy and data protection is incorporated as a matter of fundamental rights in the European Convention of Human Rights (Art.8), Lisbon Treaty (Art. 16) and the Charter of Fundamental Rights of the EU (Art. 7-8).

8 European Union, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32018R1807

Finally, the third model is based on controlled data transfers. This model is more common among countries where the concept of the right to privacy is relatively recent.[9] Countries following this model tend to link data privacy to cybersecurity, given that, generally, data regulation is elevated to a matter of national security (e.g. see Gao, 2019),[10] and implement extensive restrictions on cross-border data transfers, including the local processing of data or the ex-ante authorisation by the government to transfer data abroad following a security assessment.[11] Concerning the domestic processing of personal data, some of these countries implement comprehensive data protection laws, and others do not implement these regulations. Generally, regardless of the presence of a comprehensive data protection law, these countries exercise extensive and systematic control over personal data, sometimes through indiscriminate government access to personal data justified under national security and public order (Wang, 2012; Rubinstein et al., 2014).[12]

Table 1. Main features of data models on cross-border data transfers

Open model	Self-certification; self-assessment schemes; ex-post accountability; trade agreements and plurilateral/bilateral arrangements as only means to regulate data transfers.
Conditional model	Conditions to be fulfilled ex-ante, including the adequacy of the recipient country, binding corporate rules (BCR), standard contract clauses (SCCs,) data subject consent, and codes of conduct, among other conditions.
Control model	Strict conditions including bans to transfer data across borders; local processing requirements: ad hoc government authorisation for data transfers; infrastructure requirements; ex-ante security assessments.

Source: Ferracane and van der Marel (2024).

Until the year 2000, all African countries followed an open model for cross-border data flows as a result of the general lack of regulation in this area. This picture remained mostly unchanged until 2010, while the last decade witnessed significant regulatory action (Figure 1). In 2023, a total of 40 countries regulated transfers of personal data, of which 26 implemented a conditional flow model (48 per cent), whereas 14 implemented a control model (26 per cent). The rest of the countries do not impose any restrictions on the transfer of personal data (26 per cent).

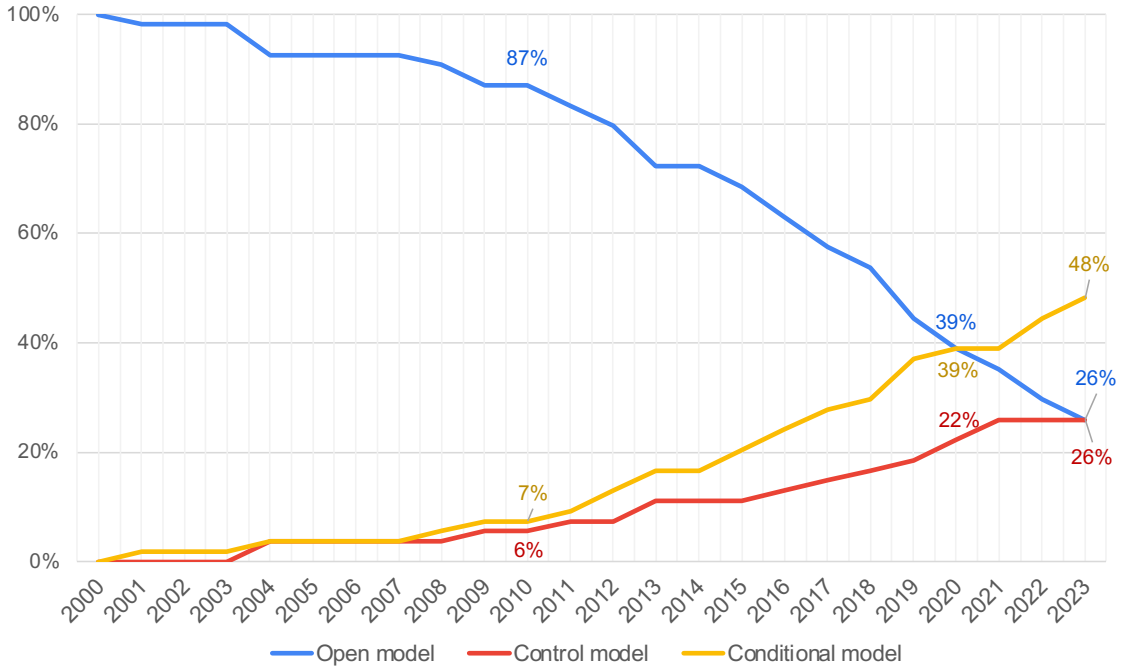
9 In China, which is the major actor employing this data model, the first mention to data privacy appeared when the Tort Liability Law was enacted in 2009 (Wang, 2012).

10 Regarding China, Gao (2019) adds that “the key to understand data regulation in China, therefore, must be security”. The heightened link with security not only explains the domestic regulatory framework in China, but also informs on how China would deal with the issue at the international level. As stated by President Xi, “there is no national security without cybersecurity”.

11 See China’s 2017 Cybersecurity Law, which imposed several restrictions aiming to “safeguard cyber security, protect cyberspace sovereignty and national security”, as stated in the Cybersecurity Law of the People's Republic of China, as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016, Art. 1, available at http://www.chinalawinfo.com. See also Gao (2019) for an analysis of the Chinese data model. Another example if the Russian Federal Law No. 242-FZ “On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks’ from 21 July 2014, which required data operators to ensure that the recording, systematisation, accumulation, storage, update/ amendment, and retrieval of personal data of the citizens of the Russian Federation is made using databases located in the Russian Federation.

12 Wang (2012) states that with respect to China: “in the constitution law, penal laws, penal litigation laws, state security laws, and other public sector laws there are many exemption rules and vague definitions that grant the government extensive rights and generous room for flexibility for investigation, seizure, and search, especially in the areas of state security or for maintaining social order”.

Figure 1. Share of countries adopting the three models for cross-border data transfers (2000-2013)

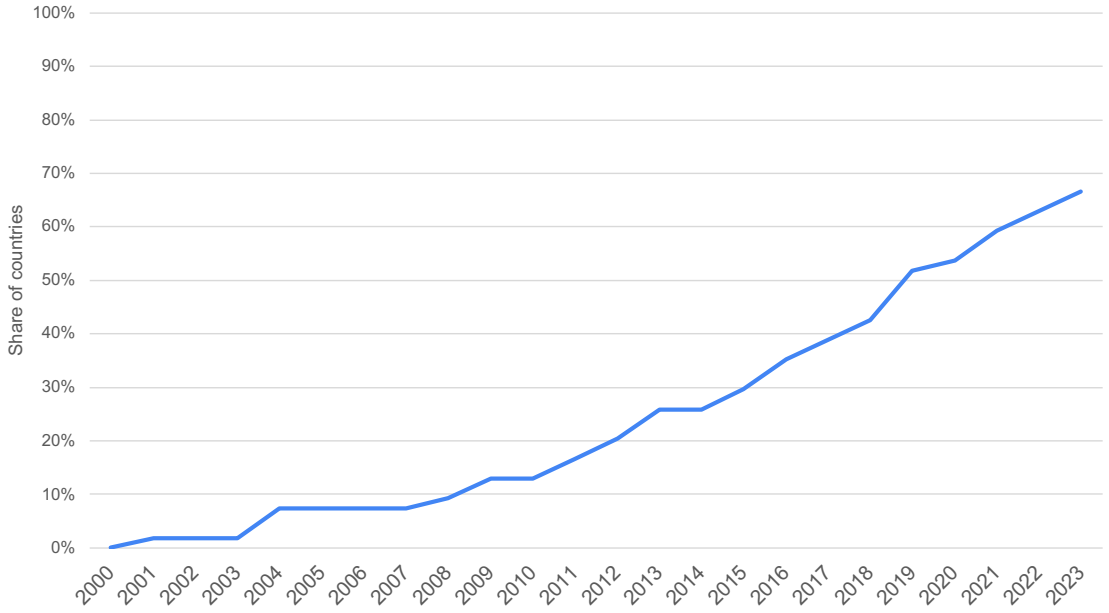


Source: Authors based on DTI database. The policies selected for the analysis are listed in Annex Table A1.

For the 54 countries in our sample, we also assess whether they have implemented a comprehensive data protection regime, that is a framework characterised by wide data subject rights, including the requirement for data subject consent for data collection and the rights to access, modify and delete personal data. In most cases, the laws also establish data protection authorities (DPAs) or agencies. When countries lack a comprehensive framework for personal data, data subjects have limited rights regarding how their data is handled. In some countries, while a horizontal data protection regime is missing, there are sectoral rules for certain sensitive categories of data, such as in finance and health.

Figure 2 shows a clear trend with a gradual increase in countries implementing comprehensive data regimes over time. By 2010, only 7 countries in the region had implemented a comprehensive regime for data protection, while as many as 36 countries had a data protection framework in place in 2023. That is, only one-third of the countries in the region lack a comprehensive regime for data protection. This trend is probably connected with the general increased interest worldwide in the issue of data protection, especially following Snowden's revelations. Most countries adopt a regime resembling the European Union's GDPR, reflecting the growing importance of the Brussels effect in the region.

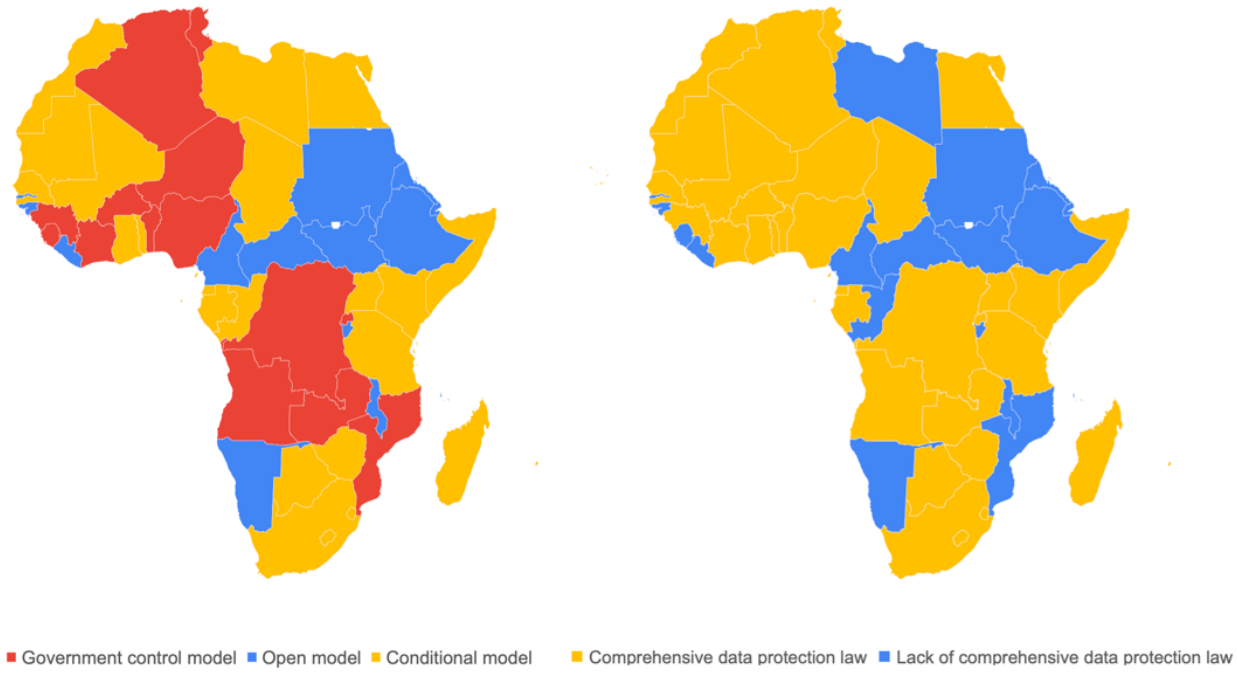
Figure 2. Share of countries adopting a comprehensive data protection regime (2000-2013)



Source: Authors based on DTI database.

As a result, the regulatory landscape for data across the African continent has become significantly fragmented, as shown in Figure 3.

Figure 3. Regulatory landscape for data models in Africa (2023)



Source: Authors based on DTI database.

As mentioned above, countries implementing a conditional model for data transfers generally do so in the context of a broader implementation of a comprehensive regime for data protection, often inspired by the European Union's GDPR. Therefore, most countries in our sample that implemented a data protection law inspired by the EU framework have also implemented a conditional regime for data transfers. Yet, this is not always the case. Some countries have implemented additional

restrictions in their data protection law that result in a control regime for data transfers, as is the case for those countries requiring the government's approval in addition to the consent of the data subjects to transfer data across borders.[13] On the other hand, countries that have not implemented any data protection law have either an open transfer of data across borders as they lack regulation in this area or, in some cases, they implement strict conditions, resulting in a control model.

4. Empirical strategy

This section presents the specification of the baseline regression using the gravity model. We start by estimating whether sharing any of the three data models correlates with greater or lower trade in digital services compared to the benchmark, which is not sharing the same data model. The empirical strategy uses a binary variable between the exporting and importing countries, varying over time, to indicate whether country pairs in our sample share the same regulatory model for data. This variable is assigned a value of one if they do and zero otherwise.

Because of its dyadic nature, this indicator resembles other conventional time-varying bilateral gravity variables, such as whether countries share an FTA or are members of the WTO. However, our indicator is more similar to the time-varying variable developed by La Porta et al. (2008), which measures whether countries share similar legal origins, categorised into French, German, and Scandinavian legal systems. Therefore, the interpretation of our variable aligns more closely with this latter work. Melitz and Toubal (2019) use this legal origin variable in a gravity model to assess whether a common legal system between partner countries impacts trade, finding a positive and significant impact.

In our baseline regression, we examine whether having a common model for data transfers and a data protection regime affects bilateral digital services trade between partner countries. In the next step, we extend this baseline regression to determine whether the results differ by type of data model.

4.1. Baseline regression

Equation (1) formally measures whether sharing the same data model for cross-border data transfers and a regime for data protection affects trade in digital services between country-pairs. Specifically, we regress bilateral trade in services sector *s* between country *o* (exporter) and country *d* (importer) over *t* (time) on our dyadic indicators, reflecting whether countries share the same data model and protection regime separately, captured by the terms *DM_odst* and *DP_odst*, respectively. Hence, the empirical baseline model takes the following form:

$$DSX\_odst = \exp\left[\theta\_1\, DM\_odst + \theta\_2\, DP\_odst + \delta\_ods + \delta\_odt + \delta\_ost + \delta\_dst\right] * \varepsilon\_odst \quad (1)$$

Our trade variable, *DSX_odst*, covers all service sectors, both digital and non-digital, varying by exporter, importer, year, and sector. Our variables of interest also vary by sector, denoted by subscript *s*, including the full range of services sectors. To capture the effect of data models on digital services, we interact the data model and protection regime indicators with a dummy variable indicating whether sector is a digital service sector. The rationale is that data policies are unlikely to affect all services sectors equally. Our identification strategy assumes that changes in data models, specifically the switch from an open to a conditional or control regime, are likely to have a disproportionate impact on sectors reliant on data. The categorisation of digital sectors is explained further in Section 3.2.

In the next step, we split the term *DM_odst* into the three different data models to study the trade effect of sharing the open, conditional, or control model for the cross-border flow of data between partner countries *o* and *d*, over time *t*. In doing so, the extended empirical baseline model formally takes the following form:

13 This is the case of Algeria, Angola, Benin, Burkina Faso, Côte d'Ivoire, Guinea, Niger, Tunisia, and Zambia.

$$DSX\_odst = exp\,[\theta\_1\,OP\_odst + \theta\_2\,CO\_odst + \theta\_3\,GC\_odst + \delta\_ods + \delta\_odt + \delta\_ost + \delta\_dst\,] * \varepsilon\_odst \quad (2)$$

OP_odst, *CO_ods*, and *GC_odst* represent the open, conditional, and control models for data, respectively. Note that we allow all three independent variables to vary by sector *s*, as we again interact the three data models with a similar dummy variable indicating whether the sector is digital or not.

The terms δ_*ods*, δ_*odt*, δ_*ost*, and δ_*dst* refer to the four sets of fixed effects applied in both equations. Respectively, they denote the exporter-importer-sector, exporter-importer-time, exporter-sector-year, and importer-sector-year fixed effects. The latter two are the widely cited multilateral resistance terms for both exporter and importer, varying by sector. The inclusion of δ_*odt* in both equations conveniently subsumes all gravity variables that vary by country-pair-year, such as sharing an RTA and WTO membership. Note, however, that due to the inclusion of our sector-level interactions, the interpretation of the empirical results slightly changes: any significant positive outcome indicates a change towards digital services trade flows relative to non-digital services trade due to the policy change. Finally, ε_*odst* is the residual term.

Admittedly, the two equations face endogeneity concerns. To address this issue and ensure our estimations are exogenous, we would need an instrument, which is very challenging in our case. Therefore, all policy variables in both Equation (1) and Equation (2) are lagged by two years to minimize any endogeneity concerns as much as possible.

The model is estimated with PPML with fixed effects following standard practice as recommended by Santos Silva and Tenreyro (2006) in addition to Baier and Bergstrand (2007), Anderson and Yotov (2016), Piermartini and Yotov (2016). By doing so, Fally (2015) shows that the estimated fixed effects correspond exactly to the terms required by the structural model. We check for possible non-existence of estimates following Santos Silva and Tenreyro (2010) and apply the procedures developed by Dai et al. (2014), which address the use of many dyadic fixed effects combined with the trend effects needed to identify the impact of time-varying policies consistently. Regressions are estimated with robust standard errors clustered by country-pair and year, following the three-way clustering approach by Egger and Tarlea (2015).

4.2. Digital service sectors

We use three measures to define digital services sectors, as there is no commonly accepted definition of digital services. All three approaches help determine whether a sector qualifies as digital and whether it is reliant on data.

First, the OECD-WTO-IMF Handbook on Measuring Digital Trade (IMF et al., 2023) categorizes digital trade into two overlapping sets of products: digitally ordered and digitally delivered trade. Given that the former is more difficult to measure, and since the Handbook concludes that only services can be digitally delivered, we focus on digitally delivered services. The Handbook defines digitally delivered services as comprising all service sectors except those closely tied to goods trade, such as transport, processing of physical inputs owned by others, maintenance and repair of goods, travel, and construction. Column (5) in Table A2 lists the services classified as digitally deliverable by the Handbook.

However, the list of digitally delivered services leaves open the question of whether some sectors are more sensitive to cost frictions related to data policies due to their reliance on data in their production models. To further narrow down this list, Ferracane and van der Marel (2021a) developed an alternative approach to defining digital services through an indicator called "data intensity." This data intensity measures the ratio of software expenditures to labour costs in USD, using data from the U.S. Census and the U.S. Bureau of Labor Statistics. Software expenditures are defined as the expenditures in Million USD for each sector, and labor costs are measured as the expenditures

on labour for each sector. The sectors with the highest ratios are telecommunications, computer services, information services, finance, and insurance. Column (6) in Table A2 reports the software-to-labor ratios for each sector.

We further refine our list of data-reliant services by identifying which sectors depend more heavily on the cross-border flow of personal data. We do so by referring to the list of companies that obtained certification under the Privacy Shield Framework (PS) maintained by the US Department of Commerce. This certification scheme allowed U.S. companies to process European citizens' data. The PS forms a legal agreement regulating the exchange of personal data flows between two of the world's largest bilateral digital service trade models: the EU's GDPR and the US's open model.[14] All companies on the PS list report their sectoral activity. We use this information to compute the share of certified companies in the total number of U.S. firms for each services sector. Data on the total number of U.S. firms is from the U.S. Census. Column (7) in Table A2 reports the shares. It shows that business services, healthcare, media and entertainment, education, and travel services are all most reliant on cross-border data flows under the PS regime.[15]

Annex Table A2 provides the final list of digital services sectors based on our three digital measures. Our selection gradually expands the scope of digital services, starting with the narrowest sectoral scope in Column (1), which includes core digital services: publishing, audio-visuals, telecom, computer services, and business services. In Column (2), we expand this definition by adding financial and insurance services, which also heavily rely on data. The third definition in Column (3) includes various personal services, and the final definition in Column (4) additionally covers charges for intellectual property rights. We use all four definitions of digital services sectors in our regressions.[16]

4.3. Trade Data

Data on bilateral trade in gross values are sourced from the WTO-OECD Balanced Trade in Services Dataset, also known as BaTiS (Liberatore and Wettstein, 2021). The primary advantage of using BaTiS is its comprehensive recording of services trade for many developing countries, including those in Africa. Another database that captures services trade flows for many developing countries is the International Trade and Production Database for Estimation (ITPD-E) from the United States International Trade Commission (Borchert et al., 2021; 2022). The difference between BaTiS and the ITPD-E is that the latter only records reported trade data, whereas BaTiS also imputes trade data using statistical techniques.

The biggest drawback of BaTiS is that many trade flows for developing countries are based on estimation procedures, including those for African countries. These estimates are derived using various methods, ranging from simple techniques like backcasting and interpolation to more sophisticated ones like gravity models. Despite this limitation, BaTiS remains the best available cross-country trade dataset for African countries to obtain probable econometric results. In fact, although ITPD-E covers an impressive array of developing countries, it has significant gaps for the African region.

Therefore, while we prefer to use data from BaTiS, it is important to note that the results of this paper should be interpreted with caution. This is despite the numerous fixed effects applied, which help eliminate standard confounding gravity factors used to estimate trade flows in the BaTiS database, which might otherwise cause biased results.

14 The European Court of Justice (ECJ) repealed the Privacy Shield agreement in 2020. In July 2023, the European Commission adopted a decision of adequacy for the EU-US Data Privacy Framework, a new mechanism replacing the Privacy Shield.

15 We manually concord the services sectors between the US Census classification system and the classification used by our trade data. A recent survey involving SMEs in four European markets shows that travel services, business services and the arts, entertainment, and recreation in the form of media and entertainment are high utilizers of personal data too (Kearney, 2021).

16 We consider all the approaches above to select the four different categorizations. For instance, even though some sectors rank high on data-intensity (S/L ratio) measure, if they are not considered as a digital deliverable service according to the Handbook by IMF-OECD-UNTAD-WTO and does not rank high in the share of firms that have signed up on the PS framework, it is not considered as digital. This is the case for the transportation sector.

5. Results

The results of the first set of regressions following equation (1) are reported in Table 2. The Table shows the coefficient outcomes for countries sharing the same data model (regardless of which one they follow) and a comprehensive data protection regime. We do not find any significant effect from sharing the same data model, which is in line with previous research. This is because the effect varies by data model, as we will show below. However, we find significant negative results from sharing the same data protection regime across all definitions of digital services, with the effect being strongest for the narrower definition (Column 1).

This means that, on average, the presence of a comprehensive data protection law between partner countries is negatively associated with intra-African trade in digital services. This finding aligns with previous studies highlighting the costs of the GDPR, which, as shown above, has heavily influenced the data protection laws in the African region (see also Makulilo, 2013). This result is also consistent with works such as Mannion (2020) and Bryant (2021), which discuss the potential negative impact of importing the EU's conditional model of regulating data protection in Africa. Yet, these findings differ from some studies that have emphasised the importance of data protection in increasing consumer trust (Zhang et al., 2020), although the evidence is not consistent (Bauer et al., 2021). Moreover, this finding differs from a previous study covering a larger group of countries, where the authors found that a domestic regime for data protection would be expected to support digital trade (Ferracane and van der Marel, 2021b; 2024).

To further investigate the negative relationship between data protection and trade in digital services, we extend the baseline regression to assess whether the effect of data protection regimes varies by income level. Since some African countries are more developed than others, we examine whether the compliance costs associated with implementing a comprehensive data protection regime disproportionately affect trade in less developed countries. In fact, developed countries, which often have more productive firms, typically find it easier to recoup the compliance costs associated with new regulations, such as a data protection regime. This could explain the positive effects of such regulations on consumer trust found in the literature.

To test this hypothesis, we categorise the 54 African countries by income groups according to the World Bank classification: high-income, upper-middle-income, lower-middle-income, and low-income. We assign country pairs to each of these four income groups and create a dummy variable that takes the value of 1 if countries share the same income group. We also do this for countries that do not fall in the same income group, which is called OT. These dummy indicators are then interacted with our dummy for sharing a data protection regime. These interaction terms measure how the negative effect of sharing a comprehensive data protection regulation varies by income group. The regression outcomes are reported in Columns 5-8 of Table 2. In the table, high-income countries are not included due to too few observations, and upper-middle-income countries are used as a benchmark.[17]

17 Note that we need to assign a benchmark, as we cannot include all four groupings. Because we expect that sharing a data protection regime is less costly for high-income countries, it seems reasonable to use this as our benchmark. However, Africa only counts three high-income groups, namely Equatorial Guinea, Mauritius, and the Seychelles, which provides few observations. Therefore, we choose to take upper-middle-income countries instead.

Table 2. Regression results following equation (1)

	(1) EXP Dig 1	(2) EXP Dig 2	(3) EXP Dig 3	(4) EXP Dig 4	(5) EXP Dig 1	(6) EXP Dig 2	(7) EXP Dig 3	(8) EXP Dig 4
Sharing data model	0.014	0.003	0.003	0.004	0.017	0.005	0.006	0.006
	(0.340)	(0.829)	(0.802)	(0.787)	(0.250)	(0.704)	(0.680)	(0.669)
Sharing data protection	-0.065**	-0.044*	-0.045*	-0.045*	0.041	0.064	0.064	0.064
	(0.014)	(0.073)	(0.067)	(0.063)	(0.507)	(0.293)	(0.292)	(0.288)
Sharing data protection * LMC					-0.053	-0.059	-0.059	-0.062
					(0.422)	(0.358)	(0.353)	(0.328)
Sharing data protection * L					-0.119**	-0.118**	-0.117**	-0.118**
					(0.036)	(0.036)	(0.036)	(0.034)
Sharing data protection * OT					-0.127**	-0.130**	-0.132**	-0.132**
					(0.042)	(0.034)	(0.030)	(0.029)
FE ods					Yes			
FE odt					Yes			
FE ost					Yes			
FE dst					Yes			
Obs	405416	405416	405416	405416	405416	405416	405416	405416

Note: p-values in parentheses * p<0.10 ** p<0.05 *** p<0.01. Robust standard errors clustered by country-pair-year. LMC = lower-middle-income countries, L = low-income countries, and OT = other income group countries, which covers country-pairs from a different income group. Middle-income countries are used as a benchmark to perform the regressions for each income group.

The results indicate that low-income countries primarily drive the negative effect observed in Columns 1-4. Their results are negative compared to the omitted group, which is the upper-middle-income countries. This negative and significant result is consistent across all four definitions of digital services. For the lower-middle-income group, the results remain insignificant. These findings align with our expectations: low-income countries face a relatively higher cost burden for firms to comply with new regulations, whereas this burden is less pronounced for more developed countries.

Furthermore, Table 2 also shows that countries not in the same income group exhibit a negative and significant result. This outcome suggests that when trading partners have different income levels, they also experience lower digital services trade compared to our benchmark of upper-middle-income countries. In other words, the negative average trade effect of sharing a data protection regime found in Columns 1-4 is not only driven by partner countries both being classified as low-income but also by those with substantially different income levels.

Our next step is to split the cross-border data model into three distinct models to study their trade effects separately. Following Equation (2), we measure whether sharing the open, conditional, or control model for cross-border data flow between partner countries is positively or negatively associated with digital services trade. The regression outcomes are reported in Table 3. The results show that the open model is positive and significant across all four definitions of digital services trade. The conditional model, on the other hand, shows a negative and significant result for all four definitions, indicating a negative association with digital services in Africa. Both results are consistent with previous studies assessing the impact of the three data models globally (Ferracane and van der Marel, 2021b; 2024).

Table 3. Regression results following equation (2)

	(1) EXP Dig 1	(2) EXP Dig 2	(3) EXP Dig 3	(4) EXP Dig 4	(5) EXP Dig 5	(6) EXP Dig 6	(7) EXP Dig 7	(8) EXP Dig 8
Sharing data model OP	0.105***	0.101***	0.103***	0.103***	0.110***	0.106***	0.108***	0.107***
	(0.002)	(0.002)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Sharing data model CO	-0.062**	-0.077***	-0.080***	-0.079***	-0.060**	-0.076***	-0.079***	-0.078***
	(0.012)	(0.001)	(0.001)	(0.001)	(0.016)	(0.001)	(0.001)	(0.001)
Sharing data model GC	0.013	-0.001	0.002	0.002	0.014	-0.000	0.002	0.002
	(0.644)	(0.985)	(0.947)	(0.949)	(0.634)	(0.990)	(0.934)	(0.934)
Sharing data protection	-0.101***	-0.084***	-0.084***	-0.085***	0.001	0.020	0.020	0.020
	(0.004)	(0.008)	(0.007)	(0.007)	(0.990)	(0.761)	(0.759)	(0.751)
Sharing data protection * LMC					-0.046	-0.052	-0.052	-0.055
					(0.489)	(0.426)	(0.418)	(0.390)
Sharing data protection * L					-0.113**	-0.110*	-0.110*	-0.111**
					(0.049)	(0.051)	(0.051)	(0.049)
Sharing data protection * OT					-0.136**	-0.138**	-0.141**	-0.141**
					(0.031)	(0.025)	(0.022)	(0.021)
FE ods					Yes			
FE odt					Yes			
FE ost					Yes			
FE dst					Yes			
Obs	405416	405416	405416	405416	405416	405416	405416	405416

Note: p-values in parentheses * p<0.10 ** p<0.05 *** p<0.01. Robust standard errors clustered by country-pair-year. LMC = lower-middle-income countries, L = Low-income countries, OT = other income group countries, which covers country-pairs from a different income group. Middle-income countries are used as a benchmark to perform the regressions for each income group.

The analysis of the control model does not yield any significant results, although the sign of the coefficient is positive, suggesting a potential positive association. This finding differs from previous studies that found a negative relationship globally (Ferracane and van der Marel, 2021b; 2024). Several explanations are possible for this discrepancy. One explanation is that political ties might play a more critical role than compliance costs for these countries, so trade is not affected by the high costs imposed by the control model. Another possibility is that the stricter requirements to process personal data locally, which define the control model, remain 'on the books' and are not enforced by companies.

6. Conclusions

In the African continent, policy discussions revolve around the benefits of a harmonised regional approach to data governance to foster trade and trust in the digital economy. This paper provides empirical evidence as to which data model would be best suited to promote digital trade in the region, both for cross-border transfers and domestic data processing.

By assessing the data models implemented by 54 African countries, we find that the EU model for regulating personal data has heavily influenced the data policies in the region, with almost half of the countries implementing conditions on data transfers and two-thirds of the countries with a comprehensive data protection law. Yet, our analysis shows that the Brussels effect does not appear to be beneficial in promoting intra-regional trade as both the conditions applied to transfers across borders and the presence of ambitious data protection regimes domestically are associated with lower intra-regional trade in digital services, although the results differ by income level.

The negative result associated with the presence of a comprehensive data protection regime diverges from previous research that shows the positive effect of these regimes on enhancing consumers' trust. We explain this difference with the fact that compliance costs derived from implementing a comprehensive data protection regime may disproportionately affect less developed countries. In fact, we find that country-pairs of low-income economies drive the negative relation, while no significant effect is found for country-pairs of middle-income economies. A negative effect is also found in the digital services trade between country-pairs from different income groups. This finding deserves further research to strike a balance between the need to protect the privacy of citizens and the need for low-income economies to enhance growth. The Malabo Convention could serve as a roadmap to advancing and harmonising a data protection policy that reflects the continent's priorities and values.[18] By creating regional alignment in the data protection laws, the Convention could enable better and faster implementation at a domestic level by fostering collaboration, mutual learning, and the development of regional best practices.

Regarding cross-border data models, we find that the conditions applied to data transfers are associated with lower intra-regional trade in digital services. This result aligns with previous studies, where the conditional model was also found to impact trade in services negatively. Contrary to several previous studies, we do not find any significant effect for the stricter control model. The explanations for this finding can be diverse. One explanation is that political ties might play a more critical role than compliance costs for these countries so that trade is not affected by the additional compliance costs. Another possible explanation is the stricter requirements to process personal data locally (that define the control model) are not enforced in practice. More research in this area would help explain these findings.

Our analysis shows, in line with previous findings, that a regime with open data transfers benefits intra-regional trade in digital services. This is the only model for which we find consistently a positive and statistically significant relation with trade in digital services. If countries in the region countries were to implement an open regime of data transfers, they could benefit from an increase of intra-regional trade in digital services by up to 11%,[19] a much-needed boost given that Africa today covers less than 1% of global trade in digitally-deliverable services.[20] This amounts to 135 million USD for intra-African trade in digital services in the region.[21]

18 African Union (2014), African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

19 This number is derived by taking the expected value: exp (0.105)−1= 11%. The value 0.105 is the average value across the results of the coefficient for the open model.

20 UNCTADstat, data for 2022, accessed in February 2024, https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices

21 According to BaTiS for which the latest year of trade data is available, based on Dig 3 definition of digital trade, total trade in digital services within Africa was 1209 mln USD * 0.11 = 135 mln USD. Dig 3 definition of digital services trade excludes IPR, health, education and other personal services.

Our findings, therefore, support the ongoing discussions in the context of the AfCFTA to foster data transfers in the region and highlight the benefits of the commitments being discussed in the Digital Trade Protocol. An explicit commitment to free transfers of data within the region as part of the Digital Trade Protocol of the AfCFTA would provide legal certainty, which should also be reflected in the agreements of the African regional economic communities (RECs) that currently restrict transfers of data outside the respective REC. These include the East African Community E-Commerce Strategy and the Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS Supplementary Act on Personal Data Protection) (Rotich, 2023).

By offering empirical evidence on the effect of regulatory policies adopted in the region, we hope to inform the policy debate in the region about the benefits and costs associated with specific regulatory policies on personal data. Yet, the definition of the regional framework for data flows and data processing that reflects the priorities and values of the region should also be informed by additional empirical evidence on the effectiveness of data policies to achieve non-economic public policy goals. In addition, additional research would be beneficial to study the potential effects of different data policies on trade between the region and the rest of the world so that both intra-regional and multilateral discussions can benefit from much-needed empirical evidence.

References

Acquisti, A., Taylor, C., and Wagman, L. (2016), "The Economics of Privacy", *Journal of Economic Literature*, Vol. 54, Issue 2, pages 442-92.

Anderson, J., and Yotov, Y. (2016), "Terms of trade and global efficiency effects of free trade agreements", *Journal of International Economics*, Vol. 99, Issue C, pages 279-298.

African Union (2014), "African Union Convention on Cyber Security and Personal Data Protection", available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union (2020), "The Digital Transformation Strategy for Africa (2020-2030)", available at https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

African Union (2022), "Data Policy Framework", available at https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf

Baier, S., and Bergstrand, J. (2007), "Do free trade agreements actually increase members' international trade?", *Journal of International Economics*, Vol. 71, Issue 1, pages 72-95.

Batikas, M., Bechtold, S., Kretschmer, T., and Peukert, C. (2020), "European Privacy Law and Global Markets for Data", CEPR Discussion Paper DP14475.

Bauer, P. C., Gerdon, F., Keusch, F., Kreuter, F., & Vannette, D. (2021), "Did the GDPR increase trust in data collectors? Evidence from observational and experimental data", *Information, Communication & Society*, Volume 25, Issue 14, pages 2101–2121.

Borchert, I., Larch, M., Shikher, S., and Yotov, Y. (2021), "The International Trade and Production Database for Estimation (ITPD-E)", *International Economics*, Vol. 166, pages 140–166.

Borchert, I., Larch, M., Shikher, S., and Yotov, Y. (2022), "The International Trade and Production Database for Estimation - Release 2 (ITPD-E-R02)", USITC Working Paper 2022–07–A.

Bradford, A. (2020), "The Brussels Effect: How the European Union Rules the World", Oxford University Press, https://doi.org/10.1093/oso/9780190088583.001.0001

Bryant, J. (2021) "Africa in the information age: challenges, opportunities, and strategies for data protection and digital rights" *Stanford Technology Law Review*, Vol 24(2), pages 389-439.

Cariolle, J., and Piedade, C. (2023) "Digital Connectedness and Exports Upgrading: Is sub-Saharan Africa Catching Up?", *The World Economy*, Vol. 46, No. 11, pages 3325–3344.

Chen, C., Frey, C., and Presidente, G. (2022) "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally", The Oxford Martin Working Paper Series on Technological and Economic Change, Working Paper No. 2022-1.

Dai, H., Milkman, K., and Riis, J. (2014), "The Fresh Start Effect: Temporal Landmarks Motivate Aspirational Behavior", *Management Science*, Vol. 60, Issue 10, pages 2563-2582.

Egger, P., and Tarlea, F. (2015) "Multi-way Clustering Estimation of Standard Errors in Gravity Models", *Economics Letters*, Vol. 134, pages 144-147.

European Union, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

Fally, T. (2015), “Structural gravity and fixed effects”, *Journal of International Economics*, Vol. 97, Issue 1, pages 76-85.

Ferracane, M.F., Kren, J., and Van der Marel, E. (2020), “Do data policy restrictions impact the productivity performance of firms and industries?”, *Review of International Economics*, Vol. 28, No. 3, pages 676-722.

Ferracane, M. F. and S. González Ugarte (forthcoming), “Data localisation: global trends”, EUI RSC Working Paper; Global Governance Programme-505; EUI.

Ferracane, M.F., and Van der Marel, E. (2021a), “Do Data Flows Restrictions Inhibit Trade in Services?”, *Review of World Economics*, Vol. 157, No. 4, pages 727–776.

Ferracane, M.F., and Van der Marel, E. (2021b), “Regulating Personal Data: Data Models and Digital Services Trade”, Policy Research Working Paper; No. 9596. World Bank, Washington, DC.

Ferracane, M. F. (Ed.). 2022. Digital Trade Integration Database. European University Institute et al. available at dti.eui.eu

Ferracane, M.F., Hoekman, B., Van der Marel, E. and Santi, F. (2023), “Digital trade, data protection and EU adequacy decisions”, EUI RSC Working Paper; 2023/37; Global Governance Programme-505; EUI.

Ferracane, M.F., and Van der Marel, E. (2023), “Digital Trade’s Regulatory Environment: Opportunities for regulatory harmonisation in Africa” UN-ECA, Addis Abeba.

Ferracane, M.F. and Van der Marel, E. (2024), “Governing personal data and trade in digital services”, Special Issue Paper, *Review of International Economics*, March 2024.

Fiorini, M., B. Hoekman, and D. Quinn (2022), “Services Trade Policy and Industry Performance in African Economies”, Robert Schuman Centre for Advanced Studies Research Paper No. RSC_75, December 2022.

Gao, H. S. (2019), “Data Regulation with Chinese Characteristics”, SMU Centre for AI & Data Governance Research Paper No. 2019/04; Singapore Management University School of Law Research Paper No. 28/2019.

International Monetary Fund, Organisation for Economic Co-operation and Development, United Nations Conference on Trade and Development and World Trade Organization (2023), “Handbook on Measuring Digital Trade, Second Edition”, OECD Publishing, Paris/International Monetary Fund/UNCTAD, Geneva 10/WTO, Geneva, https://doi.org/10.1787/ac99e6d3-en

Kearney (2021), “The economic costs of restricting the cross-border flow of data”, ECIPE and Kearney report, available at https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625036783000

La Porta, R., Lopez-de-Silanes, F., and Shleifer A. (2008), "The Economic Consequences of Legal Origins", *Journal of Economic Literature*, Vol. 46 (2), pages 285-332.

Liberatore, A. and S. Wettstein (2021), “The OECD-WTO Balanced Trade in Services Database (BPM5 edition)”, Methodology paper associated with the BaTiS database, WTO, Geneva.

López González, J., F. Casalini and J. Porras (2022), "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris, available at https://doi.org/10.1787/c5ca3fed-en

Makulilo, A. (2013), ""One size fits all": Does Europe impose its data protection regime on Africa?", *Datenschutz und Datensicherheit*, Vol. 37, pages 447–451.

Mannion, C. (2020), "Data Imperialism: The GDPR's Disastrous Impact on Africa's ECommerce Markets", *Vanderbilt Journal of Transnational Law*, Vol. 53, Issue 2.

Melitz, J., and Toubal F. (2019), "Somatic distance, trust and trade", *Review of International Economics,* Vol 27, Issue 3, pages 786–802.

Mozilla (2022), "The Malabo Roadmap: Approaches to promote data protection and data governance in Africa*",* available at: https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf

Piermartini, R., and Yotov, Y. (2016), "Estimating trade policy effects with structural gravity", WTO Staff Working Papers*,* No ERSD-2016-10*,* World Trade Organization (WTO), Economic Research and Statistics Division.

Rotich, N. (2023), "Examining Cross-Border Data Flows Provisions in Africa's Free Trade Agreements", *Strathmore University*, available at: https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/

Rubinstein, I., Nojeim, G., and Lee, R. (2014) "Systematic Government Access to Personal Data: A Comparative Analysis", *International Data Privacy Law*, Vol. 4, Issue 2, pages 96–119.

Salami, E. (2022) "Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa", *Journal of African Law*, Vol. *66*(2), pages 281–291.

Santos Silva, J., and Tenreyro, S. (2006), "The Log of Gravity", *The Review of Economics and Statistics*, Vol 88, issue 4, pages 641-658.

Santos Silva, J., and Tenreyro, S. (2010), "On the existence of the maximum likelihood estimates in Poisson regression", *Economics Letters*, Vol 107, issue 2, pages 310-312.

USITC (2019), "U.S.-Mexico-Canada Trade Agreement: Likely Impact on the US Economy and on Specific Industry Sectors", available at https://www.usitc.gov/publications/332/pub4889.pdf

Wang, Z. (2012) "Systematic Government Access to Private-Sector Data in China", *International Data Privacy Law*, Vol. 2, No. 4, pages 220-229.

World Bank (2021), "World Development Report 2021: Data for Better Lives", Washington, DC: World Bank, available at https://www.worldbank.org/en/publication/wdr2021

Zhang, J., Hassandoust, F., and Williams, J. (2020) "Online Customer Trust in the Context of the General Data Protection Regulation (GDPR)," *Pacific Asia Journal of the Association for Information Systems*, Vol. 12, Issue 1, Article 4.

Annex 1

Table A1. Data policies applied to cross-border transfers of personal data in Africa in 2023[22]

Country	Law	Description
Algeria	Law No. 18-07 Relating to the Protection of Individuals in the Processing of Personal Data (2018)	Art. 44 of Law No. 18-07 provides that the data controller may only transfer personal data to another foreign state upon authorisation of the data protection authority and if that state ensures an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing to which such data are or may be subject. Art. 45, however, provides that, by way of derogation to Art. 44, the data controller may transfer personal data to a foreign State subject to certain conditions, including: if the data subject has expressly consented to their transfer; if the transfer is made pursuant to a bilateral or multilateral agreement to which Algeria is a party; with the authorisation of the national authority; if the transfer is necessary: (a) to safeguard that person's life; (b) the preservation of the public interest; (c) compliance with obligations to ensure the recognition, exercise or defence of a legal right; (d) the performance of a contract between the controller processing and the data subject, or measures pre-contractual agreements taken at the latter's request; (e) the conclusion or performance of a contract concluded or to conclude, in the interest of the data subject, between the controller and a third party; (f) the execution of a mutual legal assistance measure international; (g) prevention, diagnosis or treatment of medical conditions. In addition, the last paragraph of Art. 44 forbids, in any case, the communication or transfer of personal data to a foreign country when this transfer is likely to harm public security or the vital interests of the state.
	Decision No. 48/SP/PC/ARPT/17 defining the conditions and modalities for establishing and operating of hosting and storage services for computerised content for user benefit in the context of cloud computing services (2017)	Art. 10 of Decision No. 48/SP/PC/ARPT/17 provides that in carrying out the activity covered by its authorisation, the service provider is subject to the obligations to establish its infrastructure on national territory and guarantee that it is set up using equipment incorporating the most recent and proven technologies; to guarantee that customer data is hosted and stored on national territory; to provide services via infrastructures specifically declared for this authorisation; to guarantee a back-up solution for data hosted or stored; and to keep a customer identification file. Service provider refers to any natural or legal person who has been granted authorisation to establish and operate hosting and storage services for computerised content for the benefit of remote users as part of cloud computing services, in compliance with the requirements set out in the legislation and regulations in force.

22 The information is sourced from the DTI database which contains information on 54 African economies. The data on African countries has been collected in collaboration with UN-ECA.

Angola	Law No. 22/11 on the Protection of Personal Data (2011)	Under Section VI of Law No. 22/11, a conditional flow regime is established for the transfer of personal data outside Angola. This means that international data transfer can only proceed if certain conditions are met. The law outlines two main scenarios for international data transfer: - If the country the data is being transferred to can guarantee an adequate level of protection of personal data, then a notification to the Agência de Protecção de Dados (APD, Data Protection Agency) is sufficient to proceed with the transfer, as per Art. 33; - If the country does not provide adequate protection of personal data, then the data controller must obtain authorisation from the APD before proceeding with the transfer, as per Art. 34. However, the APD has not issued any decision declaring countries adequate and as a result, the authorisation remains currently the only means for transfer. Art. 24 states that the interconnection of data may only be carried out with the authorisation of the APD, unless otherwise provided by law. The APD only authorises such interconnection if it is appropriate for the pursuit of the lawful purposes of data processing. Interconnection of data is defined as a form of processing of personal data consisting of the possibility of linking the data in one file with the data in other file(s) kept by another controller or by the same controller for other purposes. As a result, this requirement likely affects cross-border transfers.
Benin	Law No. 2009-09 Dealing with the Protection of Personally Identifiable Information (2009)	Section 43 of Law No. 2009-09 provides that the transfer of personal data to another country or an international organisation requires prior authorisation from the Regulator.
	Law No. 2017-20 of 20 April 2018 on the Digital Code in the Republic of Benin (2018)	Art. 391 of Law No. 2017-20 requires that the transfer of personal data to a third State or international organisation may only take place when the Authority finds that the State or international organisation in question ensures a level of protection equivalent to that provided for in the law. Art. 392 provides some exceptions, including the express consent of the data subject and the necessity of the transfer for the execution of the contract.

Botswana	Data Protection Act (2018)	Section 48 of the Data Protection Act (DPA) prohibits the transfer of personal data from Botswana to another country, unless the personal data that is undergoing processing or intended processing is transferred to a third country which ensures an adequate level of protection. Such level of protection will be assessed by the Commissioner in light of all the circumstances surrounding the data transfer operation in accordance with Sections 49 (1)-(4). Alternatively, the transfer is allowed if there is the consent of the data subject or where the transfer is: necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre-contractual measures taken in response to the data subject's request; necessary for the performance or conclusion of a contract in the interests of the data subject between the data controller and a third party; necessary for the public interest, or for the establishment, exercise or defence of a legal claim; necessary to protect the vital interests of the data subject; or made from a register that is intended to provide the public with information and is open to public inspection. In addition, Section 20 of the DPA prohibits the processing of sensitive personal data except under certain circumstances. These include: the processing is specifically provided for under the DPA; the data subject has given consent in writing; the data subject has made the data public; the processing is necessary for national security, for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, or where the processing is authorised by any other written law for any reason of substantial interest to the public; or the processing is necessary to protect the vital interest of a data subject and another person in a case where consent cannot be given by or on behalf of the data subject, the data controller cannot be reasonably expected to obtain consent or the consent by or on behalf of the data subject has been unreasonably withheld. It is not clear whether a data transfer is considered a form of processing.
Burkina Faso	Law No. 001-2021/AN protecting people with regard to the processing of personal data (2021)	According to the Art. 42 of Law No. 001-2021/AN, international transfers cannot be made without the respect of the following conditions: - a request for authorisation of the Commission For Information Technology and Civil Liberties (CIL); - a signature of a data confidentiality clause and a data reversibility clause in order to facilitate the complete migration of the data at the end of the contract; - the implementation of technical and organisational security measures. Additionally, the transfer can only be made to a foreign country or an international organisation if the recipient country or international organisation ensures an adequate level of protection equal to the one ensured in Burkina Faso. In addition, according to the Art. 37, health data allowing the direct or indirect identification of individuals must be stored on national territory. An exception can be granted if the Commission For Information Technology and Civil Liberties (Commission de l'Informatique et des Libertés, CIL) ensures that the use of information and communication technologies for the purpose of processing personal data does not pose a threat to individual or public freedoms and privacy (Art. 56).
Cape Verde	Law No. 133/V/2001, of 22 January: establishes the general legal regime for the protection of personal data of natural persons (2001)	Art. 19 of Law No. 133/V/2001 provides that transfer of personal data outside of Cabo Verde is only permissible if the foreign country ensures an adequate level of protection. However, according to Art. 20, the transfer of personal data to a country which does not ensure an adequate level of protection may be permitted by Comissão Nacional de Proteção de Dados Pessoais (CNPD, National Commission of Data Protection) if the data subject has given consent to the transfer or under limited exemptions provided for by the law.

Chad	Law No. 007/PR/2015 on the Protection of Personal Data (2015)	Art. 29 of Law No. 007/PR/2015 on the protection of personal data prohibits the transfer of personal data to a country that is not a member of the Economic and Monetary Community of Central Africa (CEMAC) or the Economic Community of Central African States (ECCAS), unless that state ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals. Certain exceptions apply (Art. 30-33). Prior to any transfer of personal data abroad, the data controller is required to inform the regulatory authority, the National Agency for Information Security and Electronic Certification (ANSICE). In addition, processing of special categories of data (including sensitive data) is prohibited unless consent of the data subject is obtained (Chapter V). According to Art. 52, authorisation of the ANSICE, is mandated to process this data. It is not clear how this requirement affects the capacity of companies to transfer data across borders.
Congo	Law 29-2019 on the Protection of Personal Data (2019)	Law No. 29-2019 states that the transfer of data abroad is possible if: the third country ensures a sufficient level of protection of privacy, fundamental rights and freedoms of people (Art. 23); the person to whom the data relates has agreed to their transfer; the transfer is necessary to protect that person's life; to safeguard the public interest; and the execution of the contract between the interested party and the data manager (Art. 24).
Côte d'Ivoire	Law 2013-450 on the Protection of Personal Data (2013)	Under Art. 26 of Law No. 2013-450, the controller of a processing operation may only be authorised to transfer personal data to a third country if that country ensures a higher or equivalent level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing of which such data are or may be subject. In addition, before any actual transfer of personal data to this third country, the controller must first obtain authorisation from the Protection Authority. The transfer of personal data to third countries is subject to regular monitoring by the Protection Authority with regard to their purpose.
DRC	Law No. 20/017 on telecommunications and information and communication technologies (2020)	Art. 132 of Law No. 20/017 provides that the collection, recording, processing, storage and transmission of personal data shall be carried out with the authorisation of the user concerned or of the competent public authority. Moreover, it is prohibited the collection and processing, which, according to the definition, includes the transfer, of personal data revealing the racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic data or more generally data relating to the state of health of the person concerned. Art. 2 states that Law No. 20/017 applies to the various activities of the telecommunications and information and communication technologies sector on national territory, and it also applies to any processing of personal data by a natural person or legal entity under public or private law, and by the public sector.
Egypt	Resolution No. 151 of 2020 approving the Law on the Protection of Personal Data (2020)	Art. 14 of Law No. 151 of 2020 on Personal Data Protection prohibits the transfer of personal data to a foreign country unless the laws of the foreign country guarantee a minimum level of protection that is equal to the level stipulated by Egyptian law. Moreover, the transfer of data abroad requires an authorisation or a licence from the Data Protection Centre. Art. 15 enumerates several specific exceptions to the obligation of Art. 14 subject to the express consent of the person concerned with the data or his representative.

Equatorial Guinea	Law No. 1/2016 on the Protection of Personal Data (2016)	Arts. 27 and 28 of Law No. 1/2016 provide that organizations may not transfer any personal information to countries that fail to provide a legally equivalent level of protection, unless the transfer has been previously authorized by the Governing Body for the Protection of Personal Data or under some exceptions, such as consent or contractual necessity. It is reported that the Governing Body for the Protection of Personal Data has not yet been established and there is no list of legally equivalent countries.
Eswatini	The Data Protection Act No. 5 (2022)	Section 32(1) of the Data Protection Act provides that if a Southern African Development Community (SADC) Member State has transposed the requirements under the SADC Model Law on Data Protection, the transfer of data is permitted. SADC is an economic block covering 16 countries in Southern Africa. Moreover, the transfer is permitted where the recipient establishes that the data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of the data controller or where the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the Member State (Sections 32(1)(a) and (b)). In addition, Section 33 of the Act permits the transfer of personal information to other recipients if an adequate level of protection is ensured in the country and the data is transferred solely to permit processing authorised by the controller. Apart from the above requirements, transfers of personal data are permitted where the data subject has unambiguously given their consent to the proposed transfer, the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken in response to the request of the data subject, among others (Sections 33(4)(a-f)).
Gabon	Law No. 001/2011 on the Protection of Personal Data (2011)	According to Art. 94 of the Data Protection Law, the transfer of personal data to another country is prohibited unless the destination country ensures an adequate level of privacy protection, and protection of fundamental rights and freedoms of individuals with regard to the processing operation. Determination of adequacy is a prerogative of the Gabon Data Protection Authority (the Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP)), taking into consideration the following factors: the legal provisions existing in the country in question; the security measures enforced; the specific circumstances of the processing (such as the purpose and duration thereof); and the nature, origin, and destination of the data. As an alternative to the 'adequacy' criteria, data controllers may transfer data if the data subject has consented expressly to its transfer; the transfer is necessary to save that person's life; the transfer is necessary to safeguard a public interest; the transfer is necessary to ensure the right of defence in a court of law; or the transfer is necessary for the performance of a contract between the data subject and the data controller, at the request of the data subject, or for the performance of a contract between the data controller and a third party in the interest of the data subject (Art. 95). In addition, Art. 47 of Chapter IV prohibits collecting or processing sensitive data (that is, data which reveal racial or ethnic origins, political, philosophical, or religious opinions or trade union membership of data subjects, or which relate to their health or sex life) barring certain exceptions, such as under explicit consent of the data subject as guided by the law, and when it serves the purposes of preservation of life.

Ghana	Data Protection Act (2012)	The Data Protection Act does not contain specific provisions on the transfer of personal data yet the principles relating to data processing are also applicable to the transfer of data. Section 20 requires that a person must not process personal data without the prior consent of the data subject unless the purpose for which the personal data is processed is necessary for the purpose of a contract to which the data subject is a party, authorised or required by law, to protect a legitimate interest of the data subject, necessary for the proper performance of a statutory duty, or necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied. On the other hand, Section 27 provides that a data controller who intends to process personal data must register with the Data Protection Commission. An application for registration as a data controller has to be made in writing and must contain, among other things, the name or description of the country to which the applicant may transfer the data (Section 47).
Guinea	Law No. L/2016/037/AN on cybersecurity and personal data protection in the Republic of Guinea (2016)	According to Art. 28 of Part II of the Law L/2016/037/AN, the transfer of personal data is subject to prior authorisation from the personal data protection authority. Any transfer of such data is subject to strict and regular control by the authorities with regard to their purposes. The authorisation is always needed, though other conditions must also be fulfilled. A controller of personal data may only transfer such data to a third country if the state ensures a higher or equivalent level of protection of privacy, fundamental freedoms and rights of individuals with regard to the processing to which such data may be subject.
Kenya	The Data Protection Act (2019)	Art. 48 of the Data Protection Act No. 24 of 2019 states that a data controller or data processor may transfer personal data to another country only where the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data. Alternatively, data can be transferred if the transfer is necessary for: the performance of a contract; for any matter of public interest; for the establishment, exercise or defence of a legal claim; in order to protect the vital interests of the data subject or of other persons; or for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects. Art. 49 highlights safeguards prior to transfer of personal data out of Kenya, which include: (1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards; (2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests; (3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.
Lesotho	Data Protection Act (2012)	Lesotho's data protection law allows cross-border data transfers, which are regulated as transfer of personal information outside Lesotho under Section 52 of the Data Protection Act, 2011. The transfer of personal information abroad is permitted when the laws of the destination country are substantially similar to the information protection principles under the Data Protection Act of Lesotho, or one of the other conditions is met (e.g., the data subject consents to the transfer or the transfer is necessary for the performance of a contract between the data subject and data controller). Private sector safeguards, such as binding corporate rules, may also be put in place.

Libya	Law No. 6-2022 on Electronic Transactions (2022)	According to Art. 78 of Law No. 6/2022 on Electronic Transactions, the transfer of personal data to a foreign country is only allowed if the appropriate level of data protection is considered, particularly the nature and source of the personal data and the purpose and duration of the transfer. Also, the applicable international obligations and laws and national data protection procedures of the country to which the data is transferred must be considered.
Madagascar	Law No. 2014 - 038 on the Protection of Personal Data (2015)	According to Art. 20, any personal data may be transferred only to countries that have legislation ensuring a level of protection for individuals similar to that provided by Malagasy law. Exceptionally, and with the agreement of the Malagasy Commission on Information Technology and Liberties (CMIL), the transfer of personal data is possible when the data controller presents sufficient guarantees for the protection of privacy and the fundamental rights and freedoms of individuals. In addition, it is also permitted when the individual concerned gives his/her full consent when it is in his/her interest or for the performance of a contract concerning that individual. The processing of sensitive data (racial origin, biometric data, genetic data, political opinions, religious or other beliefs, trade union membership and data relating to health or sex life) is prohibited. Derogations exist when guarantees of appropriate processing are provided to the Malagasy Commission for Computer Liberties (Art. 18).
Mali	Law No. 2013/015 on the Protection of Personal Data in the Republic of Mali (2013)	According to Art. 11 of Law No. 2013-015, Mali authorises the transfer of personal data to a foreign State when: the receiving State ensures a sufficient level of protection of individuals, indicated by the Authority in charge of the protection of personal data, due to its domestic legislation or commitments made at the international level and that these measures are effectively implemented; by decision of the Authority in charge of the protection of personal data, when the transfer and processing by the recipient of the personal data ensures a sufficient level of protection of privacy, as well as of the fundamental rights and freedoms of individuals, in particular, due to the contractual clauses or internal rules to which it is subject. In addition, pursuant to Art. 9, the processing of sensitive data, understood as any data of a personal nature relating to religious, philosophical, political, or trade union opinions or activities, sex, race, health, social measures, prosecutions, and criminal or administrative charges, is prohibited. However, sensitive data may be processed with appropriate safeguards defined by the Authority in charge of personal data protection if the data is necessary or used to safeguard the person's life, used by a non-profit organisation, or in the context of a judicial action. Processing of personal data is defined as any operation or set of operations carried out by means of automated or non-automated processes and applied to data, such as collecting, exploiting, recording, organising, storing, adapting, modifying, retrieving, saving, copying, consulting, using, communicating by transmission, disseminating or otherwise making available, bringing together or interconnecting, as well as blocking, encrypting, deleting or destroying personal data.

Mauritania	Law No. 2017-020 on the protection of personal data (2017)	Law No. 2017-020 provides that the controller may transfer personal data to a third country only if that country ensures an adequate level of protection (Art. 20). The Personal Data Protection Authority shall publish and maintain a list of states that it considers to provide an adequate level of protection (Art. 21). If the country is not included in the list of adequate countries, the controller must first inform the Authority. Moreover, Art. 24 specifies that the data controller may transfer personal data to a third country that does not meet the requirements of Art. 21, if the transfer is one-off, not massive and the person to whom the data relates has expressly consented to its transfer, or if the transfer is necessary for any of the following purposes: to safeguard the life of that person; to protect the public interest; to comply with obligations to establish, exercise or defend a legal claim; the performance of a contract between the controller and the data subject. Lastly, the Authority may authorise, on the basis of a duly motivated request, a transfer or a set of transfers of data to a third country that does not ensure an adequate level of protection, when the data controller offers sufficient guarantees with regard to the provisions of this law, including through contractual clauses (Art. 25).
Mauritius	Data Protection Act (2017)	Under Section 36(1) of the Data Protection Act, a data controller may transfer data abroad only under certain conditions. These include the compliance with appropriate safeguards, the explicit consent of the data subject and other cases of necessity of the transfer. Under Section 36(4) of the Data Protection Act, the Data Protection Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as the Data Commissioner may determine. It is reported that the authorities are yet to enforce these principles.
Morocco	Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data (2009)	According to Art. 43 of Law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data, the transfer of personal data to a foreign country is only allowed if the country offers an adequate level of protection of the privacy and fundamental rights and freedoms of individuals. In the Decision No. 236-2015 of 18 December 2015, the Moroccan data protection authority (CNDP) recognised the following countries as offering an adequate level of data protection: Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom. The transfer of personal data to a country that does not provide an adequate level of data protection is only allowed subject to the certain conditions, including the express consent of the data subject or if the transfer is necessary to safeguard the data subject's life, to safeguard the public interest, to comply with judicial obligations, for the performance of a contract between the controller and the data subject or pre-contractual measures taken at the request of the latter. Personal data may also be transferred if the transfer is carried out pursuant to a bilateral or multilateral agreement to which Morocco is a party, or with the express and reasoned authorisation of the CNDP when the personal data processing guarantees a sufficient level of protection of privacy and of the fundamental rights and freedoms of individuals, in particular, because of the contractual clauses or internal rules to which it is subject.

Mozambique	Decree No. 66/2019 of 01 of August - Telecommunications Network Security Regulation (2019)	According to Art. 7 of the Telecommunications Network Security Regulation, personal data of the residents in Mozambican territory must be stored within national borders and governed by the jurisdiction of Mozambique. However, the network and public telecommunications service operator can store consumer data in the cloud, outside of the territorial space, provided it ensures that the personal data storage is subject to the national jurisdiction and it is made available to the authorities upon request.
Niger	Law No. 2022-059 relating to the protection of personal data (2022)	According to Arts. 62 and 63 of Law No. 2022-059, transfer of personal data outside the country is subject to authorisation from the Haute Autorité de Protection des Données Personnelles (HAPDP or High Authority of Personal Data Protection). Apart from the condition of authorisation from the HAPDP, there are other conditions to be fulfilled, including that transfer can only be conducted to a country that guarantees a sufficient level of security or, if that condition is not met, that some conditions are fulfilled such as the authorisation by the owner of the data, the necessity of the transfer for health or juridical procedure, among others.
Nigeria	Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) (2013)	The National Information Technology Development Agency (NITDA) released guidelines on Nigerian content development in information and communications technology, subsequently amended in 2019. One of the requirements in Section 13.1 (2) is that "data and information management firms", both foreign and domestic, are required to store all data concerning Nigerian citizens in Nigeria. It is reported that these requirements raise costs for foreign businesses seeking to invest in the Nigerian market and create an intractable barrier to market entry for firms that distribute their data storage and processing globally. Further, such requirements prevent Nigerian businesses from taking advantage of cloud computing services supplied on a cross-border basis.
	- Nigeria Data Protection Act (2023) - Nigeria Data Protection Regulation (2019) - Nigeria Data Protection Regulation 2019: Implementation Framework (2020)	Sections 41(1) and 43(1) of the Data Protection Act (DPA) provide that a data controller is allowed to transfer personal from Nigeria to another country as long as there is an adequate level of protection of personal data in such country or the data subject consented to the transfer after being informed of the risk and did not withdraw the consent, the transfer is necessary for the performance of a contract to which the data subject is a party, the transfer is for the data subject's benefit, necessary for a public interest, necessary for legal action, or protect the vital interest of the data subject or third party. Prior to the DPA, the Nigerian Data Protection Regulation, 2019 (NDPR) was the go-to regulation on data protection. Although enforceable, it remains a subsidiary legislation, and there was no specific commission to oversee data protection. According to Section 2.11 of the NDPR, personal data transfers are permitted on condition that the destination country offers an adequate level of data protection. Determining the level of data protection is a prerogative of the National Information Technology Development Agency (NITDA) based on the Honourable Attorney General of the Federation's (HAGF) consideration of the foreign country's legal system, the rule of law, respect for human rights and fundamental freedoms, as well as relevant general and sector-specific legislation in public security, defense, national security, and criminal law. The countries whose levels of personal data protection is considered adequate are provided in the whitelist in Annex C of the Implementation Framework of the Data Protection Regulation and include 42 countries in addition to the EU Member States and all African countries who are signatories to the Malabo Convention 2014. Where a transfer to a jurisdiction outside the whitelist is being sought, the Data Controller shall ensure there is verifiable documentation to conduct the transfer under one or more of the exceptions stated in Art. 2.12 of the NDPR. These include the consent of the data subject and the necessity for the performance of the contract.

Rwanda	Regulation No. 001/R/ TD-ICS/RURA/016 OF 06/05/2016 Governing Telecom Network Security in Rwanda (2016)	Art. 16 of the Regulation Governing Telecom Network Security of 2016 restricts telecommunication service providers from transferring, storing or processing subscribers information outside of the Republic of Rwanda. In 2017, Rwanda's telecommunications regulator fined MTN Rwanda (a subsidiary of South Africa's MTN Group) USD 8.5 million (10% of its annual turnover) for failing to process Rwandan customer data in the country by transferring it to Uganda and for running its information technology services outside Rwanda.
	Law No. 058/2021 Relating to the Protection of Personal Data and Privacy (2021)	Art. 48 of the Law relating to Protection of Personal Data and Privacy outlines a set of conditions required to be met by a data controller or data processor in order to transfer personal data outside Rwanda. These include: - Authorization from the Supervisory Authority; - Consent by the data subject; - Performance of a contract; - Public interest grounds; - Defense claim; - Protection of vital interests of data subject; - Legitimate interests by the data controller; - Performance on international instruments ratified by Rwanda. Art. 50 clarifies the first condition stating that all personal data must be stored in Rwanda unless the company has a valid registration certificate authorising it to store personal data outside Rwanda, which is issued by the National Cyber Security Authority.
Sao Tome and Principe	Law No. 03/2016 - Aims to Guarantee and Protect the Personal Data of Individuals (2016)	According to Art. 19 of Law No. 03/2016, cross-border transfer of personal data is only permitted to countries considered to provide adequate levels of protection, as determined by the National Data Protection Agency (ANPDP). However, according to Art. 20, the transfer to a legal system that does not ensure an adequate level of protection may be carried out by notifying the ANPDP, or is permitted where the data subject has given his/her consent; - the transfer is necessary for the performance of a contract between the data subject and the controller; - the transfer is necessary for the performance of a contract entered into in the interest of the data subject between the controller and third party; - the transfer is necessary or required by law for the protection of an important public interest, or for the declaration, exercise or defense of a right in legal proceedings - the transfer is necessary to protect the vital interests of a data subject; or - the transfer is made from a register which, according to the laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest provided conditions laid down in the law for consultation are fulfilled in each case. In addition, the ANPDP may authorise a transfer or a set of transfers of personal data to a jurisdiction which does not ensure an adequate level of protection, provided that the controller ensures adequate mechanisms to ensure the protection of privacy and the fundamental rights and freedoms of persons and of their performance, in particular by means of appropriate contractual clauses.

Senegal	Law No. 2008-12 Concerning Personal Data Protection (2008)	Law No. 2008-12 lays down the principle that data may only be transferred to a third country if that country ensures a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals. The adequacy of the level of protection is assessed under Senegalese law (Art. 49 of the Personal Data Act). Conditions also apply to the local exporter who, under Arts. 50 and 51, may transfer data to a third country that does not guarantee a sufficient level of protection, subject to certain safeguards such as the consent of the data subject, the necessity of the transfer, etc.
Seychelles	Data Protection Act (2023)	Section 47 of the Data Protection Act provides that personal data shall not be transferred outside Seychelles unless the data processor in the recipient country or territory ensures a comparable level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. In addition, the Commission may authorise the transfer of personal data to another country provided that the recipient country is part of a cross-border privacy rules system that ensures that: a) cross-border rules system standards are legally enforceable against the data controllers and data processors as part of the certification system; b) data controllers and data processors have implemented security measures using a risk-based approach proportional to the probability of the threat and severity of the harm, the confidential nature of the information processed and the number of data subjects affected. The Commission may prohibit the transfer of data under this section as may be necessary in the public interest. Additional restrictions apply to certain categories of data. Section 22 establishes that processing of personal data relating to race, ethnic origin, biometrics, genetics, political opinions, religious or philosophical beliefs or for the purpose of identifying a person's health or sex life is prohibited, but some exceptions apply including in case of consent of the data subject. In addition, under Section 24, processing of personal data relating to criminal convictions and offences or related security measures based on the principles for lawful processing under this Act shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of a data subject. Moreover, Section 47(3) provides that personal data of Seychellois citizens pertaining to minors shall only be processed and transferred subject to the following: there is a designated data controller accountable for cross-border data processing in Seychelles; the transfer is made between intra-group schemes and the headquarters is located outside Seychelles; the data controller or data processor has informed the data subjects about the location of the data processing and all other relevant information as specified under Section 27; the transfer is necessary to protect vital interests of the data subject. In addition, Section 23 states that no person shall process the personal data of a child below the age of 18 years unless consent is given by the child's parent or legal guardian. The data controller shall obtain consent from the parents or legal guardians or verify that consent has been given in the case of data obtained from third parties, taking into account available technology.
Sierra Leone	Telecommunications Subscribers Identification and Registration Management Regulations (2020)	Section 19(1-2) of the Telecommunications Subscribers Identification and Registration Management Regulation empowers the National Telecommunications Commission to establish and maintain a central electronic database of communications service subscribers, in which all subscribers' information shall be stored. The database shall be housed either within the Commission or in another location as may be determined by the Commission. As Section 22(3-4) provides that the transfer and utilisation of subscribers' data outside the country are subject to specific approvals, it is expected that the location of the central electronic database should be in the territory of the country.

Somalia	Data Protection Act - Law No. 005 (2023)	Art. 30 of the Data Protection Act provides that a data controller may not transfer personal data to a country outside the country unless one of the following conditions is met: - the personal data will be received solely in country/ies that provide an adequate level of protection; - the recipient is an international organisation whose policies and administrative and technical measures afford an adequate level of protection; - the recipient is subject to a law, binding corporate rules, contractual clauses, code of conduct, certification mechanism or other measure that affords an adequate level of protection; or - the transfer meets one of the several criteria in Art. 31, which include, for example, consent or that the processing is necessary for the entering into or performance of a contract with the data subject.
South Africa	Protection of Personal Information Act 4 (2013)	South Africa has implemented a conditional flow regime that takes inspiration from the European model. According to the Protection of Personal Information (POPI) Act 4 of 2013, Chapter 9, Art. 72, data can be transferred to third countries only when: - the recipient is subject to a law, binding corporate rules or a binding agreement that: » upholds principles for reasonable processing of information that are substantially similar to the conditions contained in POPI; and » includes provisions that are substantially similar to those contained in POPI relating to the further transfer of personal information from the recipient to third parties who are in another country; - the data subject consents to the transfer; - the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; and/or - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and: » it is not reasonably practicable to obtain the consent of the data subject to that transfer, and » if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.
Tanzania	The Personal Data Protection Act No. 11 (2022)	Sections 31 and 32 of the Personal Data Protection Act permit the transfer of personal data outside Tanzania only on the following circumstances: a) to a country with an adequate personal data protection legal system (i.e. essentially equivalent levels of protection to that within Tanzania) provided the recipient has proven (i) such transfer is necessary for important reasons of public interest or any other legitimate purpose or (ii) the importance of the transfer and there is no reason to assume that the subject's legitimate interests may be prejudiced by the transfer or processing in the recipient country. The data collector or processor must carry out a prior data protection impact assessment on the need to transfer personal data and ensure the recipient of the data only processes the relevant information in the data and for the purpose for which the data was transferred; b) to any other country with appropriate safeguards on the security and protection of personal data provided the data is transferred to be processed for a purpose approved by the data subject, unless the data subject has consented to such transfer, or the transfer is necessary: - For the performance of a contract between the data subject and the data collector or the implementation of pre-contractual measures taken at the request of the data subject. - For the conclusion or performance of a contract concluded or to be concluded in the interest of the data subject between the collector and another person. - For any public interest or the establishment, exercise or defence of a legal claim. - To protect the vital interests of the data subject. - In accordance with a law aimed at giving information to the public which affords an opportunity for public consultation in general or anyone with a legitimate interest to submit their comments in accordance with a procedure laid down by law.

Togo	Law No. 2019-014 Relating to the Protection of Personal Data (2019)	Art. 28 of Law No. 2019-014 on the protection of personal data clearly states that data can only be transferred if the third country ensures an adequate level of privacy protection. Art. 29 admits a transfer of data provided that the transfer is one-off, not massive and that the person to whom the data relates has expressly consented to its transfer or if the transfer is necessary under specific conditions. Moreover, in Art. 30, the Data Protection Authority may authorise the transfer of data if the data controller provides sufficient guarantees with regard to the protection of privacy, fundamental rights and freedoms of the persons concerned and the exercise of the corresponding rights. In addition, in accordance with Art. 21, the processing of sensitive data is prohibited as a matter of principle. This includes all personal data relating to racial or ethnic origin, religious, philosophical, political or trade-union opinions or activities, sex life, health, social measures, prosecutions or criminal or administrative sanctions (Art. 4). However, this prohibition does not apply when, for example: the processing relates to data manifestly made public by the data subject; the data subject has given his or her consent in writing to such processing, in accordance with the texts in force; the data processing is necessary to safeguard the vital interests of the data subject or of another person in the event that the data subject is physically or legally incapable of giving consent; the processing is necessary for the establishment, exercise or defence of legal claims (Art. 22). Processing is defined as any operation or set of operations provided for in Art. 2 of this law, whether or not carried out using automated processes, and applied to data, such as collection, exploitation, recording, organisation, conservation, adaptation, modification, extraction, storage, copying, consultation, use, communication by transmission, dissemination or otherwise making available, alignment or combination, as well as the blocking, encryption, erasure or destruction of personal data (Art. 4).
Tunisia	Organic Act No. 2004-63 on the Protection of Personal Data (2004)	Pursuant to Organic Act No. 2004-63, the transfer of personal data is generally prohibited or subject to strict measures. According to Art. 52, prior authorisation from the Tunisian Data Protection Authority (Instance Nationale de Protection des Données à caractère Personnel, INPDP) is required in all circumstances. In addition, according to Art. 50, it is forbidden to transfer personal data to a foreign country where this is likely to harm the public security or vital interests of Tunisia. Lastly, according to Art. 51, the transfer of personal data is not permitted to countries which do not provide an adequate level of data protection. It should be noted that Art. 22 provides that the natural person or the legal representative of the legal entity wishing to carry out the processing of personal data and their agents must meet the following conditions: be of Tunisian nationality; be a resident of Tunisia; and have no criminal record. These conditions also apply to the subcontractor and its agents.
Uganda	- Data Protection and Privacy Act (2019) - Data Protection and Privacy Regulations, (2021)	Section 19 of the Data Protection and Privacy Act stipulates that in the event that a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller must ensure that the country in which the data is processed or stored has in place adequate measures for the protection of personal data at least equivalent to the protection provided for by this Act, or that the data subject has consented. In addition, Regulation 30 of the Data Protection and Privacy Regulations provides further details, including that any personal data processed outside Uganda shall not be further transferred to, or processed in, a third country without the express consent of the data subject.

Zambia	The Data Protection Act No. 3 (2021)	Section 71 (1) of the Data Protection Act allows for the transfer of personal data outside Zambia, except sensitive personal data, on condition that: - The data subject has consented; and the transfer is made subject to standard contracts or intra-group schemes that have been approved by the Data Protection Commissioner; or the Minister has prescribed that the transfer outside the Republic is permissible. - The Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity. Consideration by the Minister to sanction the cross-border transfer of personal data is based on the adequate level of protection, having regard to the applicable laws and international agreements in the destination country; and that the enforcement of data protection laws by authorities with appropriate jurisdiction is effective (Section 71 (2)). In addition, Section 70(3) states that "sensitive personal data shall be processed and stored in a server or data centre located in the Republic". Sensitive personal data is defined in Section 2 of the Act as personal data which by its nature may be used to suppress the data subject's fundamental rights and freedoms and includes: the race, marital status, ethnic origin, or sex of a data subject; genetic data and biometric data; child abuse data; a data subject's political opinions; a data subject's religious beliefs or other beliefs of a similar nature; whether a data subject is a member of a trade union; or a data subject's physical or mental health, or physical or mental condition. Section 14 of the Act prohibits the processing of sensitive personal data unless it is necessitated by legal claim or judicial function in court, or in the context of health service provision, or for reasons of public interest. In health service provision, the law requires that data be processed by or under the responsibility of a professional, subject to secrecy and other obligations imposed by any law or professional bodies regulating them. While data processed to serve the public interest can only be processed where adequate measures to safeguard the rights and freedoms of the data subject have been put in place.
Zimbabwe	Data Protection Act (2021)	Sections 28 and 29 of the Data Protection Act establish a framework for the cross-border transfer of data. Data can be transferred to countries that offer adequate protection. In addition, data can be transferred if it is in the public interest to do so. The data subject must provide consent to their information being transferred. However, this consent may also be implied or offered ambiguously. Moreover, Section 11 prohibits the processing of sensitive personal information unless with the consent of the data subject or where processing is for legitimate purposes. Sensitive data, according to Section 3 includes social, political, cultural information, as well as health and genetic information, and any information which may be considered as presenting a major risk to the rights of the data subject.

Table A2. Definitions of digital services

Sector description	Dig 1	Dig 2	Dig 3	Dig 4	Digitally deliverable	S/L ratio	Share PS
Telecom, computer, and information	●	●	●	●	Yes	4.10	2.59
Other business services	●	●	●	●	Yes	1.08	0.08
Insurance and pension services		●	●	●	Yes	2.88	0.05
Financial services		●	●	●	Yes	2.87	0.05
Heritage and recreational services			●	●	Yes	0.54	0.09
Trade-related services			●	●	Yes	0.51	0.02
Charges for the use of IPR				●	Yes	-	-
Health services				●	Yes	0.22	0.04
Education services				●	Yes	0.28	0.11
Other personal services				●	Yes	0.09	-
Manufacturing services					No	-	-
Maintenance and repair					No	-	-
Transport					No	0.58	-
Travel					No	0.04	0.08
Construction					No	0.06	0.00
Government goods and services					No	-	-
Services not allocated					No	0.18	-

Authors

Martina F. Ferracane

European University Institute

Martina.Ferracane@eui.eu

Simón González Ugarte

European University Institute

simon.gonzalez@eui.eu

Erik van der Marel

European Center for International Political Economy (ECIPE)

erik.vandermarel@ecipe.org