Enabling policy frameworks for digital and data services for expanded economic growth and development – a focus on the SADC Region

AUDA-NEPAD
AFRICAN UNION DEVELOPMENT AGENCY

Further together
vodacom

Notice

This paper has been prepared by Cliffe Dekker Hofmeyr Inc ("Cliffe Dekker Hofmeyr") for Vodacom Group Limited in accordance with the mandate concluded between them and specifically for the purposes of providing information to enable regulators and policy makers in the SADC region to understand international and regional regulatory and policy developments relating to digital, cloud and data services and to explore potential gaps and opportunities in local laws, regulations and policies allowing for cross border data transfers to facilitate digital, cloud and data services.

Cliffe Dekker Hofmeyr accepts no responsibility or liability to any party other than Vodacom in respect of this paper or any of its contents. It should not be used for any other purpose or in any other context.

This report contains various facts, statements and also includes views and suggestions which are specifically based on the research and analysis conducted within the agreed parameters, limits and context of the mandate and are generally accurate up to the date of finalisation of the research on this report, being July 2022. However, as there has been a proliferation in the number of developments in various countries over the last few months, in both the regulatory and policy space relating to the digital economy, data and cloud services and data protection, the contents of this report is only accurate and up to date up to the aforementioned date.

Use of this report

Cliffe Dekker Hofmeyr Inc is an incorporated legal practice registered in the Republic of South Africa with registration number 2008/018923/21 with its registered office at 1 Protea Place, Sandown, Johannesburg, 2196.

Executive summary

The growth of the digital economy is one of the most important developments in recent times. The **Covid-19** pandemic has caused **more than half of the world to use online products and services**[1]. The developments have underpinned exponential growth in the production and use of data globally.[2]

Stephen Chege
Group Chief Officer
External Affairs

Online marketplaces and global payment networks have allowed any business, with access to a digital platform, to reach consumers around the globe and to easily provide goods and services to them. The accessibility of a company's products and services across a range of digital platforms increasingly represents a key predictor for a business's success and an important opportunity for small and micro-sized enterprises across Africa. This in turn can be a key driver for the digital economy and related growth. Internationally, the ability to transfer, store and process data across borders has been estimated to have increased global GDP by 10.1% over the past decade.[3] However, African countries are not realising the full socio-economic benefits of the digital economies due to low levels of data protection laws and regulations, as well as the slow pace of developing and enacting them in some cases. The slow adoption and enactment of data privacy laws may contribute to a lack of trust in the security of the technology being deployed, inhibiting adoption.

An enabling regulatory environment for digital, cloud and data services that ensures appropriate free flow of data between jurisdictions should be a priority for any country which has its development as a viable digital economy as a key objective. The importance of free data flows within the context of the Fourth Industrial Revolution and its unique economic value cannot be overemphasised. The enablement of secure and easily facilitated cross-border data flows is a strong predictor for African Union ("AU") Member States to successfully compete in the global economy and thrive in a post-COVID-19 world.

In considering the inherent complexities of transferring, storing and processing data with the need to ensure the adequate protections of consumers and businesses alike, it is proposed that this may be achieved, initially in the Southern African Development Community ("**SADC**"), in the following ways:

- accelerated implementation of the principles of Africa's regional economic integration framework (under the African Economic Community("**AEC**")[4]) and exploiting its benefits such as increased economic investment and outputs, reduced regulatory barriers, economies of scale, intra-industry trade etc., to realise the operationalisation of regulatory frameworks that enable secure and easily facilitated cross-border data flows;

AUDA-NEPAD – Vodacom Public-Private Partnership Initiative

This white paper is part of the broader collaboration between AUDA-NEPAD and the Vodacom Group on strengthening the digital capabilities of AU Member States for enhanced public service delivery. Private engagements are key element in AUDA-NEPAD delivery model. Agenda 2063 is clear and resolute on the principle that sustainable economic growth and inclusive development can only be realized through mutual public-private collaboration and shared responsibilities. It is perfectly possible to pursue business interests and development at the same time; in fact, the two reinforce each other. The partnership is key for harnessing innovations that leverages on emerging data and electronic 4IR technologies to demonstrate clear and tangible value both on the business side as well as on the socio-development side.

The Vodacom Group has expanded global linkages to further enhance its outreach and operations to institutions in Africa towards building and scaling-up the digital economy. Building on AUDA-NEPAD strengths in science-based information, knowledge, expertise, and Vodacom's technological efficiencies, the linkages and proficiency open new doors of opportunities for collaborations in the digital, cloud and data services capabilities.

Executive summary

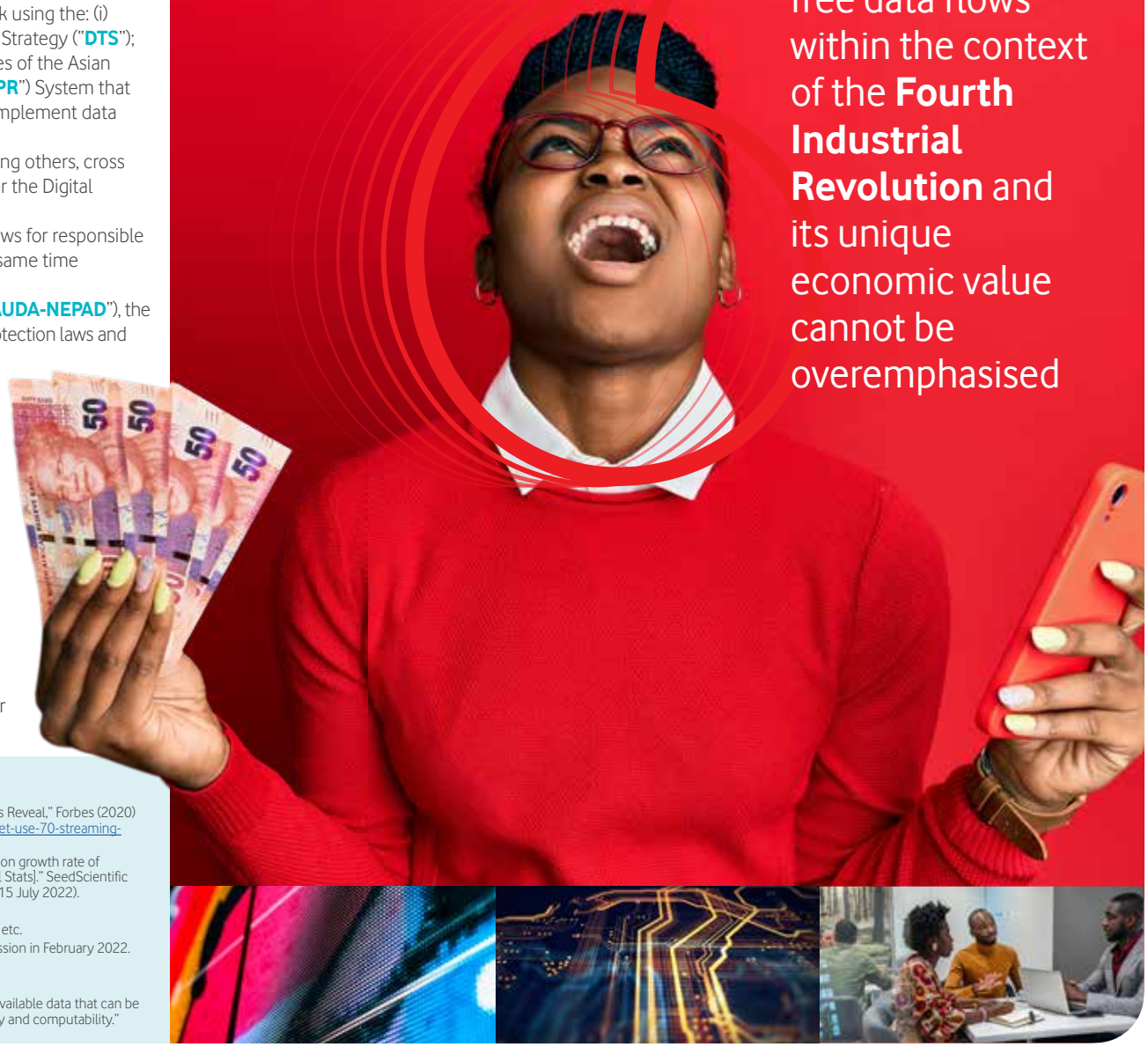
continued

- regional cooperation through policies, such as implementing a framework using the: (i) African Continental Free Trade Area ("**AfCFTA**") (ii) Digital Transformation Strategy ("**DTS**"); and (iii) Data Policy Framework ("**DPF**")[5] and learning from the experiences of the Asian Pacific Economic Cooperation ("**APEC**") Cross-Border Privacy Rules ("**CBPR**") System that applies in the APEC region which requires participating organisations to implement data privacy policies consistent with the APEC Privacy Framework;[6]
- regional cooperation by entering into trade agreements to allow for, among others, cross border data transfers, such as the Australian-Singaporean approach under the Digital Economy Agreement ("**DEA**");[7]
- regulatory reform through effective data protection legislation which allows for responsible use of data including through digital, cloud or data services, while at the same time providing adequate protection and safeguards for such data use; and
- working with AU organs such as the African Union Development Agency ("**AUDA-NEPAD**"), the AfCFTA Secretariat and the private sector to develop and/or amend data protection laws and regulatory frameworks to harness the full potential of data services and digital economies at large.

We have looked at: (a) how these mechanisms work in a number of countries and regions around the world; (b) countries that have enabling data protection policies and regulations in place, particularly to deal with enabling digital markets, cross-border data transfers and the use of new technologies; and (c) the concepts of open data[8] and data localisation, with a specific focus on how SADC countries may look at:

- addressing adequacy requirements under data protection laws (applicable to cross-border data transfers); and
- achieving standardisation in the use of terminology in laws and relevant policies.

Although the focus of this paper is the SADC region, the above approach can also be further extended to apply at a pan-African level, with adaption to other Regional Economic Communities (RECs) and national governments.



Footnotes

1. Mark Beech, "COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal," Forbes (2020) available at https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=313ce78d3104 (accessed 15 July 2022).
2. Africa in particular has been exhibiting the fastest growth in this regard, with an internet penetration growth rate of 12,441% from 2000 to 2020. Vuleta, Branka. "How Much Data Is Created Every Day? [27 Powerful Stats]." SeedScientific (28 January 2021) https://seedscientific.com/how-much-data-is-created-every-day/ (accessed 15 July 2022).
3. McKinsey Global Institute, 'Digital Globalisation: The New Era of Global Flows' (2016).
4. The AEC is the base framework that enacted the establishment of the RECs such SADC, ECOWAS etc.
5. The DPF was approved by the Executive Council of the African Union during its 40th Ordinary Session in February 2022.
6. Details are included at paragraph 5.5.
7. Details are included at paragraph 5.5.
8. The International Open Data Charter (www.opendatacharter.net) defines open data as "publicly available data that can be universally and readily accessed, used and redistributed free of charge. It is structured for usability and computability."

Introduction

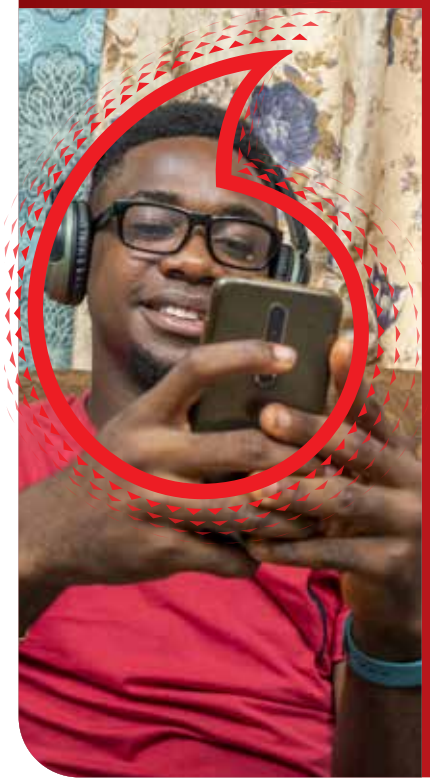
The growth of the digital economy is one of the most important developments in recent times. **The Covid-19 pandemic has caused more than half of the world to use online products and services.**[9]

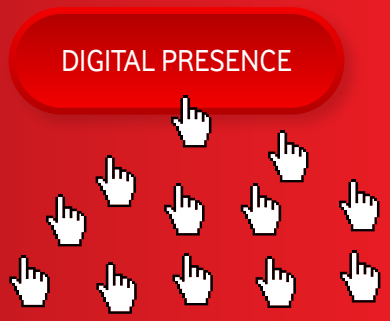
Cisco's Visual Networking Index (VNI) predicts that global internet traffic will have increased 127-fold between 2005 and 2021. By 2023, nearly two-thirds of the global population will have Internet access, which will include 5.3 billion total Internet users (66 percent of the global population), up from 3.9 billion (51 percent of the global population) in 2018.[10] **These developments have underpinned exponential growth in the production and use of data globally.**[11] For instance, the amount of data produced globally is expected to increase from 15.5 zettabytes (in 2015) to over 180 zettabytes (in 2025).[12]

Before the internet, the only companies that could access the global marketplace were those large multinational companies that were able to spread their production and sales across the world. This has changed with the rise of the digital economy. Online marketplaces and global payment networks have allowed any business, with access to a digital platform, to reach consumers around the globe and to easily provide goods and services to them. **A company's physical presence is no longer important to a consumer. Instead, the accessibility of that company's products and services across a range of digital platforms increasingly represents a key predictor for a business's success and this represents massive opportunities for small and micro-sized enterprises ("SMEs").** This in turn is likely to be a key driver for the digital economy and other related growth. Internationally, the ability to transfer, store and process data across borders has been estimated to have increased global GDP by 10.1% over the past decade.[13] **However, African countries are not realising the full socio-economic benefits of the digital economies due to low levels of data protection laws and regulations, as well as the slow pace of developing and enacting them in some cases. The slow adoption and enactment of data privacy laws may contribute to a lack of trust in the security of the technology being deployed, inhibiting adoption.** Other challenges have been the slow pace of technology adoption in Africa over the years. It has been argued that the pace of adoption could be quickened through capacity strengthening, technology transfer, international cooperation, partnerships and enabling regulations.

The enablement of secure and easily facilitated cross-border data flows is a strong predictor for AU Member States to successfully compete in the global economy and thrive in a post-COVID-19 world. According to an analysis by McKinsey, aptly titled 'Globalisation for the little guy, online marketplaces are transforming the way SMEs connect with their customers and suppliers globally.

According to a National Bureau of Economic Research ("NBER") working paper dated April 2020,[14] it is estimated that more than 100 000 small and micro-size enterprises closed from March to April of 2020. Those without a digital presence – nearly 40% – are struggling to survive. As a result, businesses must be encouraged to embrace digitisation in order to continue trading. Governments should therefore be considering how they may be able to create legal and regulatory environments that enable this process.





Without the processing and analytics capacity necessary to generate timely and accurate insights, data on its own has limited value. This is why data sharing and flows are important, as they create insights that benefit the end consumer by addressing their specific needs. Data insights allow for the roll-out of better products and services, and this, turn, benefits the business providing these products and services. The knock-on effect is obvious: thriving businesses (especially SMEs) drive growth within a local economy.

For instance, the launch of the eFounders Fellowship Programme, a partnership between UNCTAD and the Alibaba Business School in 2017, has, as of 2019, produced 122 fellows that are spread over

17 African

countries and who have created 3,400 direct jobs on the continent and generated US$100 million in annual revenues. These have mostly stemmed from start-ups and SMEs that function within the heavily data reliant industries of e-commerce and fintech services.

According to Facebook, the number of SMEs that use its platform has more than doubled in the past five years, increasing from 25 million users to over 50 million users. The Dialogue, an emerging public-policy think-tank in India, released a report stating that India may incur almost a 1% point loss in GDP in the short and medium-term if the country goes ahead with implementing restrictive cross-border data transfer laws.[15] According to a GSMA study for Brazil, Indonesia and South Africa, it is estimated that emerging economies could reap major gains from deploying Internet of Things ("IoT") technologies in conditions that are conducive to open cross-border data flows.[16] The study suggests that open cross-border data flows could have a considerable impact on economic output, in the form of increases in:

- **GDP:** up to 0.5 per cent in Brazil, up to 0.9 per cent in Indonesia, and up to 2.6 per cent in South Africa;
- **Exports:** up to 2.4 per cent in Brazil, up to 2.9 per cent in Indonesia, and up to 3.1 per cent in South Africa; and
- **Employment:** up to 0.2 per cent in Brazil, up to 0.4 per cent in Indonesia, and up to 1.3 per cent in South Africa.[17]

An enabling regulatory environment for digital, cloud and data services ensuring a free flow of data is therefore key for unlocking digital economic growth.

Considering the inherent complexities in the transfer, storage and global processing of data, along with the need to ensure adequate protections of consumers data rights, we explore **policy mechanisms that could be effectively used to regulate digital, cloud and data services and cross-border data flows in order build an enabling environment,** allowing for the digital economy to thrive across the SADC region and beyond.

Footnotes

9. Mark Beech, "COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal," Forbes (2020) available at https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=313ce78d3104 (accessed 15 July 2022).
10. Cisco Annual Internet Report (2018–2023), White paper (2020) available at https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf
11. Africa in particular has been exhibiting the fastest growth in this regard, with an internet penetration growth rate of 12,441% from 2000 to 2020. Vuleta, Branka. "How Much Data Is Created Every Day? [27 Powerful Stats]." SeedScientific (28 January 2021), https://seedscientific.com/how-much-data-is-created-every-day/ (accessed 15 July 2022).
12. "Volume of data/information created worldwide from 2010 to 2025 (in zettabytes)," (15 July 2022). https://www.statista.com/statistics/871513/worldwide-data-created/ (accessed 15 July 2022).
13. McKinsey Global Institute, 'Digital globalization: The new era of global flows | McKinsey' (2016).
14. https://www.nber.org/system/files/working_papers/w26989/w26989.pdf
15. Sharma, Aprajita. "Data Localisation May Hit GDP, Ease of Doing Business Ranking, Says Report." Business Today, 20 November 2018, https://www.businesstoday.in/current/economy-politics/data-localisation-may-hit-gdp-ease-of-doing-business-ranking-says-areport/story/292799.html. (accessed 15 July 2022). A further development is that "India and South Africa are considering blocking the renewal of a 24-year-old moratorium on tariffs on digital products such as software, movies and videos, as well as digitally enabled services, which has rattled international business groups who say the move would be a "historic setback" for the WTO", says Doug Palmer in 'India's digital tariff threat looms over WTO meeting', Doug Palmer, POLITICO Pro, 2 Jun 2, 2022.
16. Hosuk Lee-Makiyama, Badri Narayanan and Simon Lacey, "Cross-Border Data Flows The impact of data localisation on IoT" *GSMA*, January 2021, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf (accessed 15 July 2022).
17. Ibid.

Explaining cloud and data services

Cloud models

Cloud services are provided on four main types of cloud models, namely:

- public cloud;
- private cloud;
- hybrid cloud (a combination of private and public cloud); and
- distributed cloud.

Gartner defines a "**public cloud**" as computing where IT services with high elasticity and scalability are provided to external customers using internet-enabled technologies. It is typically offered as a multi-tenant environment, where the data of multiple companies or institutions can reside on the same physical server. This "pooling" of data from multiple organisations is significantly beneficial from a cost-saving perspective. The worldwide public cloud services market, including IaaS, PaaS, and SaaS (as defined and discussed below), grew 24.1% year over year in 2020 with revenues totalling $312 billion, according to the International Data Corporation (IDC) Worldwide Semi-annual Public Cloud Services Tracker.

Gartner defines a "**private cloud**" as "a form of cloud computing that is used by only one organization, or that ensures that an organization is completely isolated from others."

A **hybrid cloud** strategy is popular as it balances the advantages of both the private and public cloud and enables organisations to utilise the advantages of scaling using the public cloud's innovative and flexible services while still leveraging the customisable nature of the private cloud. According to the Flexera 2021 State of the Cloud Report, 82% of enterprises have already adopted hybrid loud strategies and an estimated growth rate of 17% has the hybrid cloud industry predicted to increase from a valuation of $44.6 billion in 2018 to almost $100 billion by 2023.

Distributed cloud is the distribution of public cloud services to different physical locations at the customer, while the operation, governance, updates and evolution of the services are the responsibility of the originating public cloud provider. Edge computing in telecommunications often referred to as "Mobile Edge Computing", "MEC", or "Multi-Access Edge Computing", provides execution resources (compute and storage) for applications with networking close to the end-users, typically within or at the boundary of operator networks.

Edge computing can also be placed at enterprise premises, for example inside factory buildings, in homes and vehicles, including trains, planes and private cars. Several use cases (enabled by IoT, 5G etc.) may require various applications to be deployed at different sites. In such scenarios, a distributed cloud is useful which can be seen as an execution environment for applications over multiple sites, including connectivity managed as one solution. **The main benefits edge solutions provide include low latency, high bandwidth, device processing and data offload as well as trusted computing and storage**.[18]

Explaining cloud and data services continued

Cloud and data services defined

Many companies, (especially financial technology (fintech), e-commerce and insurance technology (insuretech) companies), rely more and more on remote technology such as remote cloud and data services to harness the benefits of the data-rich global economy. Cloud services include cloud computing which is a type of computing where data and programs are stored and accessed over the internet. The benefits of cloud services include flexibility and reduced time to market for delivering new services through the ability to scale, compute and storage elastically up or down very quickly without having a huge total cost of ownership ("**TCO**") and time lag. To get the full benefit of cloud, however, it needs to go hand in hand with digital enablement journeys such as DevOps and Agile.

Cloud services can be categorised into three main service layers:

- infrastructure as a service ("**IaaS**");
- platform as a service ("**PaaS**"); and
- software as a service ("**SaaS**").

IaaS is a type of cloud provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources on top of which they are able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls). **Taking into consideration TCO, Cloud IaaS is a best-case scenario when compared with traditional on-premise infrastructure investments. Aside from the TCO benefits, IaaS will provide AU Member States with the opportunities of tapping into global technical expertise, capacities (and to some extent technology/expertise transfer) that comes with establishing, deploying and using the service.**

PaaS is essentially managed platforms with the cloud service provider's ("CSP") portfolio that removes a level of both technical complexity and operational overhead for the consumers of these "platforms as a service". Within this context, the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications, and possibly, configuration settings for the application-hosting environment. PaaS may consist of managed infrastructure components such as databases (RDS), serverless (e.g lambda or functions) and could also include middleware, software development tools, business intelligence ("**BI**") services and database monitoring/managing systems.[19]

SaaS is a method of software distribution where software applications are hosted remotely by a software provider and are made available to customers over a network, who lease or rent the software application.

These hosted applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Most SaaS carriers supply a usage-based subscription on a monthly or yearly basis. Although it is a departure from the traditional approach of the more costly traditional, on-premise licensing of software programs, SaaS can provide significant cost and technological advantages.[20]

Footnotes

18. https://www.ericsson.com/en/edge-computing?gclid=EAIaIQobChMImZCj2daP9AIVi7HtCh2aWwjQEAAYASAAEgK6gvD_BwE&gclsrc=aw.ds
https://www.gartner.com/en/information-technology/glossary/distributed-cloud
19. What is PaaS? Platform as a Service | Microsoft Azure. Available at: <https://azure.microsoft.com/en-us/overview/what-is-paas/> (accessed 15 July 2022).
20. : Turco, K., 2021. Top 4 Advantages of Software as a Service (SaaS) | Technology Advice. Available at: https://technologyadvice.com/blog/information-technology/advantages-of-software-as-a-service-saas-2/ (accessed 15 July 2022).

Considering Policy and Economic Factors

With the above in mind, **the creation of effective and economically conducive policies and regulatory frameworks that appropriately regulate digital, cloud and data services and cross-border data flows should be a priority for any nation that places an emphasis on its development as a viable digital economy.** The importance of data flows within the context of the Fourth Industrial Revolution and its unique economic value cannot be overemphasised.

Despite the overwhelming evidence set out above, there is a proliferation of laws around the world that restrict the movement of data across borders and as a consequence, businesses are facing regulatory challenges when seeking to deploy or use cloud services. This stems largely from the fragmentation and the incongruence of local data protection laws (including surveillance regimes) in different jurisdictions and regions. This poses a serious threat to both the digital economy and a nation's ability to maximise the economic and social benefits that have been displayed by data-reliant technologies such as machine learning and artificial intelligence (**"AI"**).

We will convey the adverse impact of adopting protectionist and restrictive data protection laws and policies while illustrating how progressive data protection laws, regulations and policies, that encourage responsible, secure and scalable cross-border data flows, have significant economic benefits.

Unpacking data practices and regulatory approaches

There are a number of recurring themes found in data protection laws and regulations around the world. Against an analysis of SADC countries and the developments in jurisdictions such as the **European Union, Singapore, Australia, Ghana, the DRC and Nigeria,** the following regulatory elements have been identified as being the main barriers to the free flow of data across international borders:

- data localisation;
- strict adequacy requirements (i.e. the requirement that data protection laws and/or practices in third countries to which data is transferred should be equivalent to the data protection laws of the originating country); and
- inconsistent use of terminology in laws and relevant policies (i.e. a lack of standardisation).

Data localisation

Data localisation defined

Data localisation is a broad term used to describe a variety of different types of restrictions and requirements imposed by national governments and regulators which require (or have as a consequence) data originating within a jurisdiction to remain in that particular jurisdiction. Put simply, "data localisation" refers to a requirement that any entity which processes the data of a country's citizens must store and process that data on servers within that country's borders. **Data localisation restrictions act as digital walls between countries and limit the free flow of data from one jurisdiction to another.**

According to Julius Nyamwena and Pamela Mondliwa,[21] –

"The data localisation policies can take a variety of forms. Stringent data localisation requires that all data generated in a jurisdiction is stored and processed within the national boundaries. The "negative list approach" to localisation requires that data should be stored and processed within the national boundaries with exceptions in some sectors or countries where data can be stored and processed outside with a copy stored within the national boundary. The "positive list approach" allows for the appropriate free flow of data with the exception of selected sectors where data must be localised and cannot leave the country's borders."[22]

Differing approaches to data localisation

There is much debate surrounding the restrictions on cross-border data flows that emanate from stringent data localisation regulations.

The main arguments brought forward by proponents of data localisation are the protection of the domestic economy, undercutting or preventing competition from big international players.[23] The concerns relating to data privacy, surveillance, legal disclosures and guarding the sovereignty of countries generally accompany the debate for stringent data localisation measures.[24] Arguments in favour of data sovereignty laws often emphasise security concerns as a focal point for their implementation.[25]

In the absence of binding international rules on cross-border data flows, many countries incorrectly correlate data localisation as the most feasible measure to ensure the protection of their citizens' data and privacy.[26] **This is not the case. Data localisation could make data more vulnerable to security breaches, by preventing "sharding" as all information would have to be stored in one place. Sharding is a process that ensures different rows of databases are located in different servers across the world, and thus "shards" provide enough data to operate while also masking the identity of data subjects.** As such, when the core regional integration principles of the AU AEC, for reduced regulatory barriers, economies of scale etc., are implemented, the appropriate flow of data system and services across borders will aid in the operationalisation of cybersecurity frameworks for RECs such as SADC.

Concerns of hardware failures, power outages, natural disasters or large-scale outages are rendered inconsequential as most of the biggest cloud providers practice "redundancy". This means that they copy data several times and store it in many different data centres around the world. Therefore, if one server goes down, another back-up server then enables access to data files regardless.

Footnotes

21. Julius Nyamwena and Pamela Mondliwa, "Policy Brief 3: Data Governance Matters: Lessons For South Africa", The Industrial Development Think Tank (2020).
22. Ibid.
23. Chander, Anupam, and Uyên P. Lê. "Data nationalism" Emory LJ 64 (2014) 677.
24. Gurumurthy, Anita, Amrita Vasudevan, and Nandini Chami. "The grand myth of cross-border data flows in trade deals." IT for Change (2017).
25. Data sovereignty refers to the concept that the data an organization collects, stores, and processes is subject to the nation's laws and general best practices where it is physically located. In other words, this means that a business has to store the personal information of its customers in a way that complies with all the data privacy regulations, best practices, and guidelines of the host country.
26. Anne Josephine Flanagan, Nada AlSaeed, Lothar Determann and Leanne Kemp "A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy" World Economic Forum White Paper (2020).

Unpacking data practices and regulatory approaches continued

The data available to date refutes the economic argument that stringent data localisation measures attract investment, fuel innovation, protect domestic industries and create a competitive advantage for domestic companies.[27] A report from the Leviathan Security Group shows that data localisation measures raise the cost of hosting data by **30-60%**.

In a study commissioned by the European Centre for International Political Economy, compliance costs the EU economy €52 billion per year whilst the removal of the existing regulations would generate GDP gains of €8 billion per year.[28] Compounding this, increased costs of doing business raises the barriers to market entry for would-be start-ups, therefore hindering innovation, causing disruption and reducing an economy's competitiveness in the long term. **Cloud computing has reduced the cost of starting a business to as low as USD 3,000 in contrast to about USD 2 million in the 1990s.**[29]

In Africa alone, the data centre market, by investment, is expected to grow at a compound annual growth rate of approximately 15% during the period 2020 – 2026.[30] **The Africa data centre market size, by investment, was valued at USD 2 billion in 2020 and is expected to increase to USD 5 billion by 2026, growing at a compound annual growth rate of 15% during 2021 – 2026.**[31] The increasing demand for cloud-based services and modular data centre solutions among enterprises, especially in SMEs and government agencies, are expected to drive the market in Africa. It is expected that over 70% of organisations operating in the continent will shift to the cloud by 2025.[32]

Best practice for addressing data localisation

The AfCFTA framework agreement seeks to create a single integrated market across the economies of African Union member states and could be an important stepping stone towards harmonisation and standardisation in the data flows and processing space.

Adopted by SADC in 2013 to safeguard data protection rights in member states was the SADC Model Law on Data Protection (**"SADC Model Law"**), which provides for member states to adopt its principles in developing data protection laws in their respective countries. The SADC Model Law calls for wide territorial scope of applicability as it encompasses "the processing of personal data by a controller who is not permanently established in a given territory, if the means used, which can be automatic or other means, is located in that given territory", and creates a framework for cross-border data transfer both within the region and out of it. The SADC Model Law provides for a detailed regime for the cross-border export of data, by regulating both the cross-border flow of data between SADC countries that have domesticated the SADC Model Law and from the SADC to other countries, aligning to the EU model of "an adequate level of protection" being required in the destination country outside of the SADC or to a SADC country which has not enacted the SADC Model Law.

Alongside this, the African Union adopted the Convention on Cybersecurity and Personal Data Protection in 2014 and in 2010, Digital Transformation Strategy, Data Policy Framework (in 2022), the Economic Community of West African States (ECOWAS) adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS which provided for the provisions required to be incorporated into local data privacy law in each of the ECOWAS member states.[33]

On 1 April 2021, the South African Minister of Communications and Digital Technologies (**"Minister"**) published a Draft National Data and Cloud Policy (**"DCP"**) for comment, which provides an indication of the government's proposed policy regarding its approach to open data and data flows. The DCP acknowledges that the South African government's position regarding the free flow of data as set out in existing legislation, including the South African Protection of Personal Information Act of 2013 (**"POPIA"**), represents an enabling regulatory environment.[34] Furthermore, the South African government's support for controlled and secure cross-border transfer of data, particularly with countries that have comparable, adequate and reciprocal data privacy regimes, should be seen as an enabling foundation to build upon. This can be achieved by aligning the objectives of the DCP with some of the primary objectives of the AfCFTA , as well as the core principles of SADC on regional integration.

Footnotes

27. Indian Council For Research On International Economic Relations, "Regulatory Burden on Micro-Small and Medium Business due to Data Localisation Policies" Data Catalyst (2019).
28. ECPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in EU Member States (2016).
29. Pepper, R., Garrity, J., and LaSalle, "Cross-Border Data Flows, Digital Innovation, and Economic Growth." *In The Global Information Technology Report 2016 – Innovating in the Digital Economy*, edited by Silja Baller, Soumitra Dutta and Bruno Lanvin, 39-47. Cologny: World Economic Forum.
30. Reportlinker.com "Data Center Market in Africa – Industry Outlook and Forecast 2021-2026" (2021) available at https://www.reportlinker.com/p05822887/Data-Center-Market-in-Africa-Industry-Outlook-and-Forecast.html?utm_source=GNW (accessed on 15 July 2022).
31. Ibid.
32. Ibid.
33. The ECOWAS Supplementary Act established the content required of a data privacy law in each of the ECOWAS member states, including the composition of a data protection authority. Eleven of the fifteen ECOWAS member states have enacted data protection laws (being Benin, Burkina Faso, Cape Verde, Senegal, Ghana, Guinea, Ivory Coast, Mali, Niger, Nigeria and Togo).
34. The DCP does not define the term "data".

Unpacking data practices and regulatory approaches continued

In August 2019, the Nigerian National Information Technology Development Agency (**"NITDA"**) released the Nigeria Cloud Computing Policy (**"NCCP"**). The NCCP was issued in terms of Sections 6(a), (b), (c), and (i) of the National Information Technology Development Agency Act No. 28 of 2007, which mandates NITDA to issue policies, frameworks, standards and guidelines for the development of the IT industry in Nigeria. **The purpose of the NCCP is to promote the adoption of cloud computing in Nigeria, specifically amongst government and SMEs**.[35]

Both the South African DCP and the Nigerian NCCP advocate for a data classification framework, which is a tool that allows organisations to assign a classification or relative values to the type of data they process, based on the type of data in question and its sensitive or confidential nature. What is critical and worth highlighting is that the NCCP provides for an exception to the requirements to house certain classified data fields within Nigeria. **It allows such data to be accessed and used in the processing of transactions on both local and international platforms for economic, developmental and policy purposes.** This, therefore, amounts to an express set of justifiable limitations with a view to enabling international and regional trade.

AU Member States can also learn from the experiences of data flow regulatory frameworks from the ASEAN region and Europe. For instance in Singapore, the approach to cross-border data flows as it relates to cloud services is one of the most exemplary of the international comparators mentioned above. **Singapore does not impose any data localisation requirements but instead opts for the adequacy requirements approach. Notably, it expressly utilises "specified certification" as an indicator of adequacy as it relates to the recipient's data protection and security obligations.** We will elaborate on the "certification" mechanisms below, as the Singaporean approach should be considered for learning and adaptation when countries structure their own cross-border data flow and cloud services regulations.

Evidence of the Singaporean approach being adopted in cloud regulatory policies can be found in the EU. The EU issued the Cloud Code of Conduct under the General Data Protection Regulation (**"GDPR"**)[36] on 19 May 2021.[37] It is the first transnational Code of Conduct, which addresses cloud offerings to be approved under the GDPR. It seeks to simplify cloud service users' assessment regarding whether a cloud computing-based service is GDPR-compliant. The Code of Conduct also specifically appoints an independent oversight body, SCOPE Europe, to accept evidence of compliance by way of certifications from cloud service providers.

The Code contains three levels of compliance for which cloud service providers can apply. The first level requires cloud service providers to conduct their own internal review of their conformity to the requirements and submit this to SCOPE Europe for review. **The second level** requires cloud service providers to submit evidence of partial compliance to SCOPE Europe, which it can receive from independent third parties. **The third level** requires that full compliance with the code is confirmed via third party certificates and audits.

On 7 July 2021, the European Data Protection Board ("**EDPB**") adopted Guidelines 04/2021 on codes of conduct as tools for data transfers. The aim of these guidelines is to specify the application of Article 40-3 of the GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data to third countries in accordance with Article 46-2-e) of the GDPR. The effect of the aforementioned guidelines now enables a code of conduct to be adhered to and used by controllers or processors not subject to the GDPR located in third countries for the purpose of providing appropriate safeguards to data transferred to third countries. Such controllers and processors are required to make binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the code including with regard to the rights of data subjects as required by Article 40-3.

Footnotes

35. Section 2 of NCCP.
36. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
37. Read the Belgian DPA approval decision regarding EU Cloud Code of Conduct, the accreditation decision regarding Scope Europe and the Belgian DPA's press release regarding the approval decision.

Unpacking data practices and regulatory approaches continued

As such, the EDPB has enabled the utilisation of standardised codes of conduct to alleviate the barriers to cross border data flows, while **the use of certification mechanisms is also important as they, unlike the codes of conduct, provide an immediate solution to the barriers identified above on a much larger scale.** Certain certification mechanisms will be highlighted below.

According to the World Economic Forum's 2020 whitepaper titled 'A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy', *"[f]or companies, an absence of data localization requirements is akin to having visa-free travel for their data. One still needs a passport (which is represented by the trust mechanisms discussed below), but travel is pre-authorized. Removing barriers to data flows is speedier, cheaper and more efficient than the contrary, and it is hugely beneficial in growing international business regardless of size".*

Strict adequacy requirements

Adequacy requirements defined

These refer to the required levels of data protection in a recipient country/organisation that are essentially equivalent to the country from which the data originates. Many countries allow cross-border data flows on the condition that the recipient country, territory or organisation display the same or substantially similar levels of data protection as they have in their own local jurisdiction. **Most SADC countries with data protection laws have implemented some form of adequacy requirement into these laws. There is therefore need for acceleration and increased scale of such implementation across all the countries in the SADC region.** Most of these SADC countries have generally followed the approach of the European Union ("**EU**") under the GDPR. The SADC Model Law aligns to these principles broadly, although it predates the GDPR.

In the EU, member states may freely transfer data between themselves under the GDPR framework but require that (apart from other mechanisms such as appropriate contracting mechanisms) adequacy decisions are issued by the European Commission (with binding effect for the entire EU) to a non-EU country, territory or specified sector within a third country, or an international organisation who offers an adequate level of data protection measured against the GDPR standards.[38] The adoption of such decisions involves a lengthy and complex process (including legal challenges to decisions made in this regard[39]) and is mainly the reason that currently only the following countries outside of the EU have been granted an adequacy decision:

- Andorra;
- Argentina;
- Canada;[40]
- Faroe Islands;
- Guernsey;
- Israel;
- Isle of Man;
- Japan;
- Jersey;
- New Zealand;
- Republic of Korea;
- Switzerland;
- United Kingdom; and
- Uruguay (private sector organisations).[41]

If an adequacy decision is issued in relation to a third country (i.e. a non-EU Member State), data controllers and processors are allowed to transfer personal data to any recipient in that country without restriction, subject to the GDPR. This may be a beneficial approach to fostering the free flow of data to non-EU Member States such as AU Member States.

Footnotes

38. Article 45 of the GDPR.
39. Examples include the Schrems I and II matters which dealt with whether the US law ensures adequate protection required for international transfers under EU law.
40. Partial adequacy decision based on the scope of local laws.
41. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Unpacking data practices and regulatory approaches continued

To this end, **data controllers who want to transfer data to a recipient outside of the EU have found it more difficult to effect such transfers if the recipient is within a country that has not been subject to an adequacy decision** from the European Commission. In the absence of an adequacy decision, the GDPR allows a data controller to transfer data if there are "appropriate safeguards" in place.

Differing approaches to adequacy requirements

The reliance on adequacy decisions has both a significant upside and downside when considering that only a few adequacy decisions have been issued thus far. However, the benefits of adequacy decisions far outweigh the disadvantages (which include the burdensome approval process for data protection authorities). Once a country is deemed adequate, businesses in both jurisdictions (i.e. businesses in the country granting an adequacy decision and the country receiving an adequacy decision) are left to freely transfer data between one another without the often timely and costly process of negotiating data protection provisions in contracts or even assessing the adequacy of a recipient country's data protection laws through the use of legal services.

The slow pace at which adequacy decisions are issued is a factor that may need to be improved in order to ease the financial and administrative burden on businesses. **Even when looking at the EU, it is recommended that the EU considers a more flexible approach to its standards for adequacy decisions, in order to be more accommodating to the needs of businesses and the imperative to ensure global free flow of data with trust.**

Appropriate safeguards include binding corporate rules, standard data protection clauses,[42] approved codes of conduct or approved certification mechanisms that ensure an appropriate level of data protection is available for public and private data importers.[43] These tools basically rely on a contractual commitment undertaken by a data recipient to conform to a set of obligations relating to the processing of data that comply with the provisions of the GDPR.

The use of "appropriate safeguards" can be somewhat problematic, especially when the intended recipient is subject to data protection laws that do not enable the appropriate safeguards effectively.

In other words, using safeguards such as binding corporate rules requires a high level of consistent data protection compliance and controls that, usually, must apply across the group of the intended recipient. **This can often be a point of contention from a contracting perspective as some jurisdictions may not require as high a level of compliance and the intended recipient may be uncomfortable with the consequences both from a cost of compliance and an enforcement perspective.**

Best practice for addressing adequacy requirements

In Africa, the adequacy approach is expressed in various forms. Many adopt the GDPR model – as seen by: (a) Section 72 of South Africa's POPIA; (b) Section 36 of Mauritius Data Protection Act 2017; (c) Section 48 of Kenya's Data Protection Act 2019; and (d) the Nigerian NITDA Data Protection Regulation 2019. These have comparable provisions on cross-border data transfers that mandate adequacy requirements based on commensurate data protection laws. A notable exception is, however, found in the jurisdiction of eSwatini.

In Sections 32 and 33 of the eSwatini Data Protection Bill of 2020, the provisions related to cross-border data transfers are based on the adequacy of the intended recipient country's enacted data protection and security laws/regulations. However, there is an exception that applies to countries that have transposed the provisions of the SADC Model Law on Data Protection.

Footnotes

42. New Standard Contractual Clauses ("SCCs") have been adopted by the European Commission on June 4, 2021.
43. Article 46 of the GDPR.

Unpacking data practices and regulatory approaches continued

These countries have been designated as automatically adequate and are allowed to receive data transfers if both the controller and the recipient prove to the Eswatini Communications Commission that there is a legitimate and verifiable necessity for such a transfer and that it does not disproportionately prejudice the legitimate interests of the data subject. Where the intended recipient has not adopted the SADC Model Law into its own local laws, the Eswatini Communications Commission can be approached to authorise such a transfer. **There is currently no indication as to what will be regarded as a verifiable and legitimate necessity under the eSwatini Data Protection Bill, however, the approach is notable for the fact that it displays the first example of a regional adequacy decision in Africa.**

The Eswatini approach is commendable in that it would ease the burden on the regulators or data protection authorities that have been tasked with the function of designating adequate jurisdictions. Using the adoption of a model law as an indicator of adequacy will provide data controllers with a clear indication of what is an adequate jurisdiction.

Another consideration is that many of the jurisdictions in Africa that provide for adequacy under their respective data protection laws have not as yet indicated which jurisdictions are adequate. South Africa and Angola are examples of such jurisdictions.

The notion that the GDPR may be seen as the "global standard" for what would be considered an adequate data protection law is also misleading specifically when considering the provisions of the POPIA in South Africa, as an example. POPIA expressly recognises juristic persons (e.g. companies) as data subjects, who are afforded the same protections as natural persons under POPIA. The GDPR does not have the same protections for juristic persons and is therefore technically inconsistent with POPIA.[44] This displays the issue facing many businesses across the globe. When a data protection law is confined to a particular jurisdiction, the invariable consequence is that a host of inconsistencies in standards, terminology and approaches arise, as further illustrated below.

Lack of standardisation

Standardisation defined

The third barrier hindering cross-border data flows is a lack of standardisation and an inconsistent use of terminology in data protection laws. The lack of standardisation regarding legal terminology is regularly recognised as the main barrier to transparency in data processing activities, often threatening to impinge on individuals' data rights.[45] Differences in the relative weight afforded to each of the priorities regarding the economic and political gains from cross-border data flows have resulted in a diversity of domestic rules governing the cross-border flows of information, especially when it relates to personally identifiable information.

In the EU, the recommendation of the High-Level Report on Capital Markets Union for the development of standard contractual clauses in cloud computing is another sign of the inherent lack of legal certainty regarding the obligations placed on data recipients and CSPs when contracting.

Standardisation of terminology and contractual obligations would benefit both customers and CSPs alike.[46] In 2020, the European Commission released the "European Strategy for Data", which emphasises the necessity of fostering an "ecosystem" based on accessible data.[47] The European Commission proposes concepts such as "data spaces" (including a "common European financial data space") as a mechanism to encourage uniform and transparent treatment of financial data.

Footnotes

44. See the definitions of "data subject", "person" and "personal information" in section 1 of POPIA.
45. Expert Group on Regulatory Obstacles to Financial Innovation, 30 Recommendations on Regulation, Innovation and Finance: Final Report to the European Commission (2019), pg. 63.
46. EC, Final report of the High Level Forum on the Capital Markets Union: A new vision for Europe's capital markets (2020), Recommendation on Cloud, pg.82–84.
47. European Commission, "A European Strategy for Data" COM (2020) 66, found here.

Unpacking data practices and regulatory approaches continued

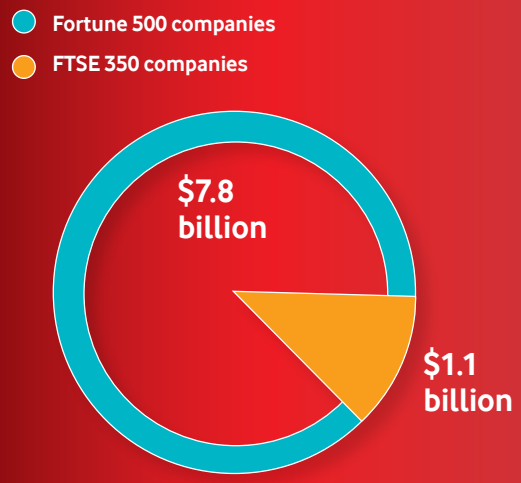
Differing approaches to standardisation

The **creation of common 'data spaces' will be expanded upon below, but, for the most part, the biggest advantage of the GDPR that should be noted is its regional application across a continent.** The advantages of a law that applies across an entire region are the consistency and standardisation emanating therefrom, as emphasised by the AU Digital Transformation Strategy and the Data Policy Framework. Consequently, the downside of the GDPR's approach is that the benefits of consistency are only utilised by the EU Member States who do not have to adopt tailored approaches when transferring data to other Member States. The drawback, however, is mostly felt by non-Member States who are left with the task of balancing their own data protection laws against the GDPR.

As a consequence, the lack of standardisation in both terminology and principles causes organisations a significant compliance burden. Forcing an organisation to ensure compliance with each of the individual data protection laws found in their various operating jurisdictions is a costly endeavour. A Forbes report found that, among Fortune 500 and U.K. FTSE 350 companies, the cost of GDPR alone is notably high, as per the illustration from that report below –

The Cost of GDPR Compliance

GDPR compliance will cost U.S. Fortune 500 and U.K. FTSE 350 companies nearly $9 billion.



DATA: International Association of Privacy Professionals (IAPP) and EY

Source: https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/?sh=6198abaa34a2

If these costs are compounded across multiple jurisdictions, organisations will find it more difficult to fully participate in a global digital economy.

Best practice for addressing standardisation practices

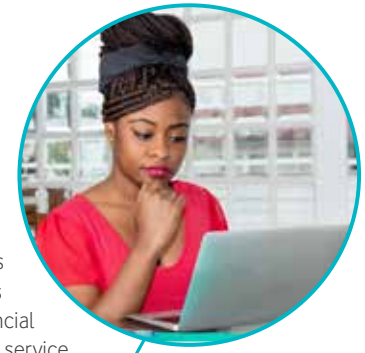
As discussed throughout this document, the effective use of regional policies, agreements and common legislation allowing for standardisation as regards the rules and procedures applicable to cross-border data flows and the use of digital, data and cloud services would allow the SADC region and the greater African continent to be at the forefront of fast-tracking realisation of the economic benefit of the digital economy.

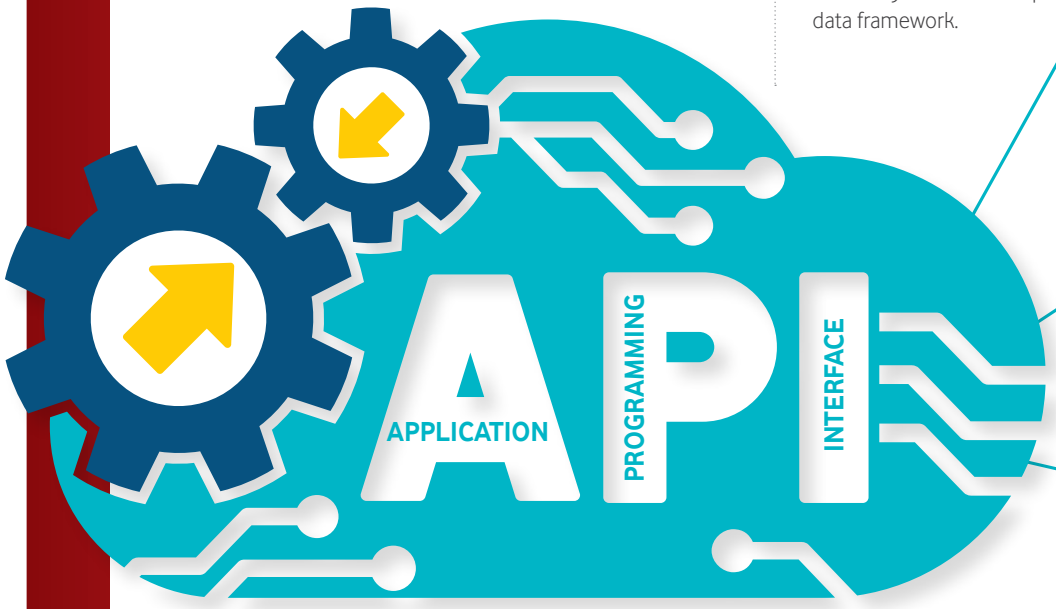
At a glance: considering global, continental, regional and country best practices

EU: Open data, PSD2 and the Single Market Approach

Open data and PSD2

An endeavour towards open data in the European Union is the Payment Service Directive 2015/2355/EC (**"PSD2"**). The PSD2 is designed to open up bank-held customer account data to Account Information Service Providers (**"AISPs"**) who have obtained the customer's consent to process such information. This concept of enabling access to data that is usually held by a bank is known as "open banking", a component of the open data concept in a specific industry. Open banking is a banking practice that provides third-party financial service providers with open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (**"APIs"**).[48] Open banking will allow the networking of accounts and data across institutions for use by consumers, financial institutions, and third-party service providers. PSD2 specifically aims to include non-banking entities into the payment industry, making a fairer playground for different players and customers alike. This is one of the key tenets of an open data framework.





The Single Market Approach

Subsequent to PSD2, the European Commission has articulated a data strategy with an aim to help grow "the use of, and demand for, data and data-enabled products and services throughout the Single Market".[49] In the eyes of the European Commission, promoting wider availability and use of data would stimulate not just "greater productivity and competitive markets, but also improvements in health and well-being, environment, transparent governance and convenient public services".[50] Two key legislative instruments that operationalise the data strategy are the 2019 Open Data Directive and the proposed regulation on European data governance (Data Governance Act). According to Boštjan Koritnik, the Slovenian Minister for Public Administration, President of the Council –

"The Data Governance Act is a major milestone that will boost the data-driven economy in Europe in the years to come. By enabling control and creating trust, it will help unlock the potential of vast amounts of data generated by businesses and individuals. This is indispensable for the development of artificial intelligence applications and critical for the EU's global competitiveness in this area. Data-powered innovations will help us address a range of societal challenges and drive economic growth, which is so important for the post-COVID recovery."

Footnotes

48. Definition of Open Banking
49. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final, Brussels 19.2.20, p. 1.
50. Ibid.

At a glance: considering global, regional and country best practices continued

As an example of an effective approach to open data, the EU Open Data Directive only applies to data that is already publicly accessible on the basis of national or EU access regimes, e.g., under laws on public registers or freedom of information acts. The Directive focuses on the economic potential of the re-use of public sector information and encourages Member States to make as much data available for re-use as possible, while also placing a particular focus on high-value data sets. High-value data sets are defined as documents whose re-use is associated with important benefits for society and the economy, such as statistics or geospatial data. These data sets are of great interest to the research community and have a high commercial potential and can speed up the emergence of a wide variety of value-added EU-wide information products and services. They also serve as key data sources for the development of AI. High-value data sets are subject to a separate set of rules ensuring their availability across the EU free of charge, in machine-readable formats, provided via APIs and, where relevant, as a bulk download.[51]

The thematic scope of high-value datasets is provided in an Annex to the Directive. The thematic categories of high-value datasets, as referred to in Article 13(1) of the Directive, are:

- geospatial;
- earth observation and environment;
- meteorological;
- statistics;
- companies and company ownership; and
- mobility.

The European Commission is working together with Member States to define a further list of specific high-value data sets and the final proposal for high-value datasets.

The proposed Data Governance Act seeks to extend the principles of the Open Data Directive to a wider range of data, which is held by public authorities but subject to third-party intellectual property rights, to commercial or statistical confidentiality, or data protection restraints. It does not oblige public sector bodies to allow re-use, but those that do must adhere to several principles. Exclusive licensing arrangements are to be avoided, and if they cannot be, they must be of limited duration (three years). Where public sector re-use is limited to certain types of uses, the conditions of each of these uses must be non-discriminatory, proportionate, and objectively justified. The charging of fees is allowed, but these must be based on the costs of processing re-use requests. As is the case in the Open Data Directive, a public sector body would be barred from exercising *sui generis* database rights to limit re-use. Of course, the public sector cannot allow the re-use of data in which third parties own intellectual property without first securing the necessary permissions. The Data Governance Act does not propose rights on access to data, although we might see those as part of the prospective Data Act,[52] which will aim to clarify who can use and access what data for which purpose for EU consumers and businesses alike. It will essentially complement the Data Governance Act in this regard.

Footnotes

51. However, according to Article 14(3), these datasets cannot be made available free of charge if this would result in a distortion of the market.
52. The Commission has published its Inception Impact Assessment. Stakeholders were able to submit their comments until 25 June 2021.

At a glance: considering global, regional and country best practices continued

Convention 108 and Convention 108 +

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108[53] is a binding international instrument that protects the individual against abuses that may flow from the collection and processing of personal data and which also seeks to regulate the trans-border flow of personal data. The "modernisation" of Convention 108 was completed by the Council of Europe's Committee of Ministers, agreeing to a Protocol amending it, on 18 May 2018. The new version (called "108+" to distinguish it) requires (in the laws of acceding countries by 108+) higher standards than those of Convention 108 and are arguably a middle ground between 108 and the GDPR.[54] Since it became open for signature on 10 October 2018, new countries wishing to accede will have to accede to both Convention 108 and the amending Protocol (i.e. to 108+). As with Convention 108, its key obligation (enforceable only by diplomatic means) is that parties to 108+ commit to allowing the free flow of personal data transfers to other parties, provided those parties implement and enforce the data protection standards of the Convention, in return for the same benefit of "free flow" of personal data to their own country.

The Convention has 55 parties, with four from outside Europe (Tunisia, Uruguay, Mauritius and Senegal). **The UN Special Rapporteur on the Right to Privacy ("SRP") has recommended that all UN member states should accede to Convention 108+ and implement its provisions in their domestic law and, where possible, implement additional GDPR principles, while leaving the door open to a broader international agreement at a later date.**[55] **The EC also endorses accession to Convention 108 by countries seeking a positive adequacy assessment under the GDPR.**[56]

Continental: The AU Digital Transformation Strategy (DTS) and Data Policy Framework (DPF)

The DTS[57], adopted by the African Union in 2020 to transform African societies and economies in a manner which allows the continent and its member states to harness digital technologies for local innovation that will improve life opportunities, ameliorate poverty, reduce inequality facilitating the delivery of goods and services. Realisation of the objectives of the DTS is critical to the achievement of the African Union Agenda 2063, the pan-African strategic framework for unity, self-determination, freedom, progress, and collective prosperity, and of the United Nations Sustainable Development Goals. The DPF builds on existing instruments and initiatives such as the DTS, AfCFTA, the Policy and Regulatory Initiative for Digital Africa ("PRIDA"), the Programme for Infrastructure Development in Africa ("PIDA") etc., to guide African Union Member States in developing their national data systems and capabilities to effectively derive value from data that is being generated by citizens, government entities and industries.

SADC: Mauritius Data Protection Act and Convention 108+

From a SADC perspective, Mauritius has taken the most strides to ensure its participation in the global digital economy. The advent of the GDPR and its adequacy requirements have guided Mauritius, as a financial hub for offshore investors,[58] to incorporate the GDPR framework into its domestic laws. The Mauritius Data Protection Act, which was passed in late 2017 and came into force in January 2018, is noteworthy for its inclusion and further development of the GDPR's use of certification mechanisms.[59] Section 48 of the Mauritian Data Protection Act (**"DPA"**) makes provision for the Data Protection Office to create the technical standards for a data protection certification mechanism. A data controller or processor who seeks certification under section 48 is required to provide the Data Protection Office with all information and access to their processing activities necessary to conduct the certification procedure. Much like the GDPR, no specific certification mechanism is prescribed or mandated, however, the express provision enabling the implementation of such a certification mechanism must be noted for its ability to enable an ease of business by having a certification indicating compliance with the obligations of the DPA itself. This is a good example for peer-learning and feedback to other AU Member States.

Footnotes

53. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
54. G. Greenleaf 'Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives' (2016) 142 Privacy Laws & Business International Report, 14-17 https://papers.ssrn.com/sol3/papers. cfm?abstract_id=2892947.
55. UN General Assembly, *seventy-third session Report of the Special Rapporteur on the right to privacy*, 17 October 2018, para. 117(e) <http://www.worldlii.org/int/other/UNSRPPub/2018/11.html>; further stated in UN Human Rights Council *2019 Annual Report of the UN Special Rapporteur on the right to privacy*, para. 28 <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>
56. See GDPR Recital 105.
57. https://archives.au.int/bitstream/handle/123456789/8758/EX%20CL%201180%20XXXVI%20Annex_E.pdf?sequence=2&isAllowed=y
58. Data from the Bank of Mauritius indicate that Mauritius' total foreign direct investment inflows amounted to 21,337 million Rupees in 2019 – Bank of Mauritius, "Preliminary Gross Direct Investment Flows: 2019" (Excluding Global Business Sector)
59. The discussion of certificates can be found in Article 42 of the GDPR.

At a glance: considering global, regional and country best practices continued

From a data localisation perspective, the DPA requires data controllers processing citizens' personal data abroad to have some local presence or representative within Mauritius. Section 36 requires that a controller or processor who transfers personal data outside Mauritius must provide the Data Protection Commissioner (**"DPC"**) with proof confirming that there are appropriate safeguards in place for the protection of personal data. In order to facilitate a cross-border data transfer, controllers/processors must complete the form provided on the DPC website, detailing the appropriate safeguards that may be implemented to ensure adequate protection for the data subject's rights under the DPA. **Coupled with the use of certification mechanisms, Mauritius displays the appropriate balance between the competing interests of data protection and economic viability in policymaking.**

Furthermore, **Mauritius is one of the few countries outside of the EU to ratify Convention 108+.**[60] Being a signatory to the Convention not only assures its own citizens of the highest standards of protection available to their data, but it also provides confidence to investors looking to start data processing businesses in Mauritius and ensures that data processors operating in Mauritius can provide these services to other signatory countries. AU Member States are recommended to ratify international conventions such as Convention 108+ and create enabling environment for spawning digital businesses as well attract FDIs into the creation of cloud data centres across the continent.

Preferential Trade Agreements ("PTAs") or Trade Facilitation Agreements ("TFAs")

In the absence of globally agreed-upon norms regarding digital trade and cross-border data flows, Preferential Trade Agreements (**"PTAs"**) or Trade Facilitation Agreements (**"TFAs"**) have served as inter-governmental tools between the respective countries that allow these governments to design bespoke economically beneficial treaty agreements relating to the digital economy and cross-border data transfers.[61] **As an example of the benefits attached to utilising trade agreements that encourage free trade between nations, the U.S. International Trade Commission estimated that the North American Free Trade Agreement could increase U.S. economic growth by 0.1%-0.5% a year.**[62]

Each PTA or TFA should be structured with tiered obligations corresponding to the individual level of development of its different members. **At the core, there should be a set of commonly accepted minimum standards or basic principles. These agreements should include the following substantive content elements: freedom of data flow for the provision of covered services, investments and intellectual property rights; prohibition of data localisation requirements relating to the hardware, software or location of data storage, with narrowly defined exceptions for measures to protect data security or personal information; and a commitment for ach party to introduce or maintain its own domestic laws on privacy protection that meets certain minimum standards.**

However, while contemporary PTAs/TFAs feature a broad set of digital provisions, there remains wide variance across agreements in terms of the depth and breadth of issues covered, with many provisions framed as "best endeavours" or soft law disciplines not subject to dispute resolution mechanisms.[63] **African countries have not fully recognised the benefits of PTAs and/or TFAs. Currently, only Morocco is party to a PTA with an e-commerce chapter (with the United States).**
The European Union's Economic Partnership Agreements (**"EPAs"**) with Côte d'Ivoire and Ghana also only contain an understanding that the parties will cooperate to facilitate the conclusion of an agreement including in trade in services and electronic commerce.

Footnotes

60. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.
61. Wu, M. (2017), Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System, RTA Exchange, Geneva: ICTSD and the IDB.
62. Congressional Research Service. "The North American Free Trade Agreement ('NAFTA')," Pg 16.
63. Meltzer, J. P. (2015), "A New Digital Trade Agenda", E15 Initiative. http://e15initiative.org/publications/a-new-digital-trade-agenda/

At a glance: considering global, regional and country best practices continued

Singapore and Australia: the Digital Economy Agreement

A good example of a pro-data flow centric trade agreement can be seen between Singapore and Australia. In March 2020, Singapore's Personal Data Protection Commission (**"PDPC"**) and the Office of the Australian Information Commissioner (**"OAIC"**) signed a Memorandum of Understanding to foster closer collaboration and cooperation in safeguarding the data protection rights of Australians and Singaporeans, given the importance of data governance and cross-border data flows to global trade.[64] Following this, Singapore and Australia signed a new, binding digital agreement on 6 August 2020.[65] The DEA upgrades the digital trade provisions in the Singapore-Australia Free Trade Agreement (**"SAFTA"**). Once in force, it will amend SAFTA, replacing the e-commerce chapter with a new and enforceable digital economy chapter.

The DEA specifically includes provisions preventing unnecessary restrictions on the transfer and location of data, including financial sector data. The DEA also includes new commitments on e-invoicing and e-payment frameworks, improved enforcement and compliance provisions around online consumer protection, enhanced transparency, and greater cooperation in online safety. This is Singapore's second DEA, after signing the Digital Economy Partnership Agreement with Chile and New Zealand earlier in 2020. Through these DEAs, Singapore seeks to facilitate end-to-end digital trade, enable trusted cross-border data flows, including those which are generated or held by financial institutions, and to build trust in digital systems.

The DEAs highlights personal information protection[66] as follows –

"[E]ach Party shall adopt or maintain a legal framework that provides for the protection of the personal information of persons who conduct or engage in electronic transactions. In the development of its legal framework for the protection of personal information, each Party shall take into account the principles and guidelines of relevant international bodies, such as the APEC Cross-Border Privacy Rules *System and the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data"*[67][68].

The DEA also states that the Parties will recognise the CBPR System as a valid mechanism to facilitate cross-border information transfers while protecting personal information.[69] The APEC CBPR System is a voluntary, accountability-based system that aims to facilitate privacy-respecting data flow. The System requires participating organisations to implement data privacy policies consistent with the APEC Privacy Framework. **The APEC Privacy Framework is a set of principles and implementation guidelines that were created in order to establish effective privacy protections that specifically avoid barriers to information flows and ensure continued trade and economic growth in the APEC region.** The APEC Privacy Framework sets in motion the process of creating the APEC CBPR System, and is the reason why the APEC CBPR System uses the APEC Privacy Framework as a base for the minimum standards of compliance.[70]

Ultimately, this makes it easier for transferring organisations to comply with their obligations under both the Australian Privacy Principles and the Singaporean Personal Data Protection Act, as they can simply check and ascertain that the recipient organisation holds the specified certification. The CBPR certification simplifies matters for recipient organisations as they can now confirm that they are certified, to reassure the transferring organisation that the transfer is permissible.[71] This may remove the need for parties to contract with the recipient organisation to grant a comparable standard of protection.[72]

The CBPR System enables the essential flow of information and data across borders while at the same time providing effective protection for personal information. The System is one by which the privacy policies and practices of companies operating in the APEC region are assessed and certified by a third-party verifier (i.e., an accountability agent) and follows a set of commonly agreed-upon rules, based on the APEC Privacy Framework. By applying this commonly agreed-upon baseline set of rules, the CBPR System bridges differences that may exist among domestic data protection approaches. **To date, nine economies have joined the CBPR System: USA; Canada; Mexico; Japan; Singapore; Chinese Taipei; Australia; South Korea; and the Philippines.**[73]

Although APEC initiatives are regionally focused, they provide a basis to scale up to larger global efforts because they reflect economies at different stages of development. Expanding the CBPR System to countries outside of APEC could represent the

64. The Australian Office of the Australian Information Commissioner and the Singaporean Personal Data Protection Commission's Memorandum of Understanding: https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-ofunderstanding/mous/mou-with-pdpc/
65. Copy of the DEA available here.
66. Article 17 of the DEA.
67. Asia Pacific Economic Cooperation ("**APEC**").
68. Article 17(2) of the DEA.
69. Article 17(8) of the DEA.
70. A brief comparison between the APEC Privacy Framework and the GDPR can be found here.
71. Template contract clause for transfers of data to overseas recipients that hold CBPR certifications can be found here.
72. For data controllers, the APEC CBPR Certification represents the requirements for businesses that control the collection, holding, processing, or use of personal data and that are interested in adhering to the voluntary framework to demonstrate its commitment to privacy. The standards are available here.
73. Lawfare, "Cross-border Privacy Rules in Asia: An Overview," (2019) available at https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

At a glance: considering global, regional and country best practices continued

next step toward consistent international rules and disciplines on data flows and privacy. **Our view is that the APEC CBPR System could serve as a model framework for AU Member States concluding policies and/or FTAs or PTAs regulating cross-border data flows.** The APEC CBPR System was designed around developed and developing countries with shared regional interests or cultural norms. For this reason, it ostensibly provides Africa with a blueprint as to what could be utilised by both countries and organisations across the continent. **The inconsistencies between two jurisdictions can be remedied with a standardised certification that mandates data protection principles, which substitute and potentially enhance the shortcomings or inconsistencies of each.**

Other examples of enabling data flows through International Trade Agreements

There are other examples of supportive and enabling approaches to cross-border data flow in terms of international trade agreements:

- UK-Japan Comprehensive Economic Partnership Agreement: According to the UK's Department of International Trade, this recently agreed trade deal will "enable free flow of data whilst maintaining high standards of protection for personal data" and introduce "a ban on data localisation, which will prevent British businesses from having the extra cost of setting up servers in Japan."[74]
- UK-Australia Free Trade Agreement: The UK and Australia signed a free trade agreement in December 2021. The UK has said in a position paper that it "will seek to guarantee the free flow of data and eliminate unjustified data localisation requirements" and noted that "[e]liminating unjustified data localisation requirements further reduces costs to businesses trading overseas, which can be prohibitive for SMEs."[75] In May 2022, the UK government introduced a bill to bring Free Trade Agreements, including this agreement with Australia, into force.
- US-Japan Digital Trade Agreement ("DTA"): In the DTA, the US and Japan agreed to refrain from prohibiting or restricting cross-border transfers of information "solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of a covered person." According to the US Trade Representative, the agreement ensures "that data can be transferred across borders, by all suppliers, including financial service suppliers."[76]
- US-Mexico-Canada Agreement ("**USMCA**"): According to the US Trade Representative, this comprehensive agreement will "[e]nsure that data can be transferred cross-border, and that limits on where data can be stored and processed are minimised, thereby enhancing and protecting the global digital ecosystem." With respect to the financial services sector specifically, the USMCA includes "[u]pdated provisions to allow for the cross-border transfer of data and an updated market access obligation."[77]
- Singapore-US Joint Statement on Financial Services Data Connectivity: Among other things, "[t]he United States and Singapore recognise that the ability to aggregate, store, process, and transmit data across borders is critical to financial sector development" and agree to both oppose data localisation requirements and ensure "financial service suppliers can transfer data, including personal information, across borders by electronic means if this activity is for the conduct of the business of a financial service supplier."[78]

Singapore's other Digital Economy Agreements: Singapore has executed a Digital Economy Partnership Agreement ("**DEPA**") with Chile and New Zealand and is currently negotiating a Digital Economy Agreement with Korea and the UK. According to Singapore's Ministry of Trade and Industry, both DEPA and the Australian DEA include provisions *"to allow data to flow freely across borders and prohibit the localisation of data except for legitimate purposes such as personal data protection."*[79]

The benefits of having a favourable cross-border data and cloud services regulatory regime are evidenced by the recent increase in international investments into Singapore. Facebook's decision to open a $1.4 billion data centre in Singapore shows the country's ambitions to become a hub for innovative digital services offerings.[80]

Footnotes

74. UK Gov (2020) Press Release: UK and Japan agree historic free trade agreement https://www.gov.uk/government/news/uk-and-japan-agree-historic-freetrade-agreement.
75. UK Gov (2020) Policy Paper: UK-Australia free trade agreement: the UK's strategic approach https://www.gov.uk/government/publications/uks-approach-tonegotiating-a-free-trade-agreement-with-australia/uk-australia-free-trade-agreement-the-uks-strategicapproach.
76. US Treasury (2019): Agreement between the Unites States of America and Japan concerning digital trade https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.
77. US Treasury: US-Mexico-Canada trade fact sheet https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.
78. MAS (2020): US-Singapore Joint Statement on Financial Services Data Connectivity https://www.mas.gov.sg/news/media-releases/2020/united-states-singaporejoint-statement-on-financial-services-data-connectivity.
79. Ministry of Trade and Industry Singapore Digital Economy Agreements (mti.gov.sg).
80. Asyraf Kamil " 'Hundreds of jobs' available at Facebook's S$1.4 billion facility in Singapore slated to open in 2022" (2018) available at https://www.todayonline.com/singapore/hundreds-jobs-available-facebooks-s14-billion-facility-singapore-slated-open-2022 (accessed 15 July 2022).

Regional opportunities for Africa: unpacking the solutions

African Continental Free Trade Area (AfCFTA)

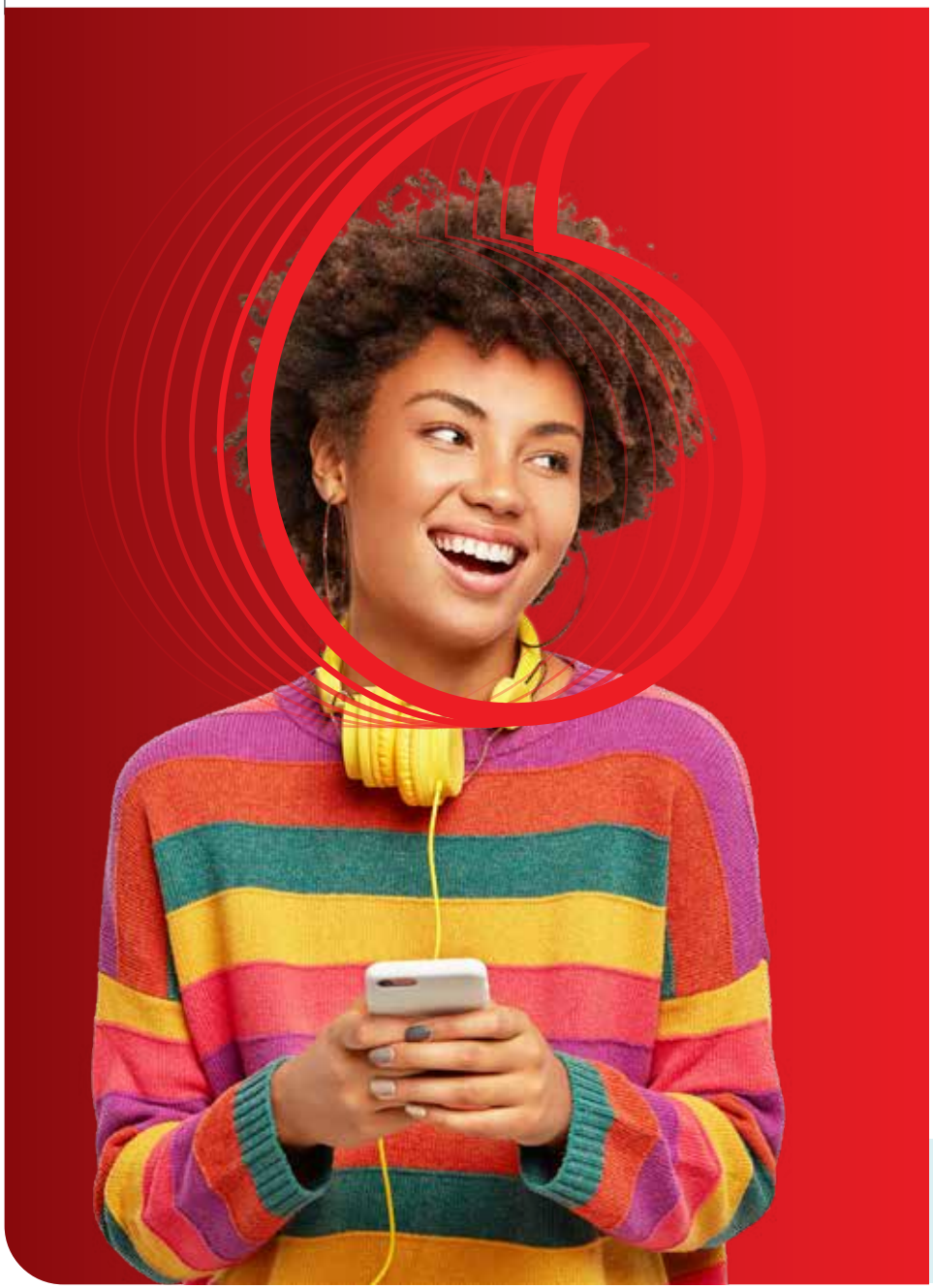
The above considerations are useful for African nations as they contemplate the normative contours of continent-wide developments on e-commerce called for under the recently established AfCFTA. The AfCFTA has a strong development focus, highlighting economic and social development and legal harmonisation among its objectives, and incorporating aspects of the African Union's Agenda 2063, which prioritises inclusive social and economic development and links Africa's growth and integration to the Sustainable Development Goals (**"SDGs"**).[81] **The AfCFTA came into effect on 30 May 2019 and features a built-in negotiating agenda on e-commerce and digital trade, while also providing AU Member States with a ready-made setting in which to implement a Pan-African digital strategy and action plans such the AU DTS and theDPF. These are aimed at accelerating the development and regulation of the continent's digital ecosystem and enhancing the volume of digitally enhanced cross border transactions.**

African Continental Free Trade Area: Implementation benefits

There are multiple benefits of the AfCFTA. We will point to two significant advantages to its implementation. **Firstly, AfCFTA will have the effect of creating a single market for goods and services to increase trading among African nations.** The AfCFTA is tasked with implementing protocols to eliminate trade barriers and cooperate with member states on investment and competition policies, intellectual property rights, settlement of disputes and other trade-liberating strategies. **Secondly, UNECA estimates that AfCFTA has the potential to boost intra-African trade by 52.3% once import duties and non-tariff barriers are eliminated.** As a single market, AfCFTA will cover a GDP of $2.5 trillion.

Footnotes

81. Agreement Establishing the African Continental Free Trade Area, Article 3, (2018) 58 I. L.M. 1028.



Regional opportunities for Africa: unpacking the solutions

continued

African Continental Free Trade Area: Rulemaking

The AfCFTA in subsequent planned phases aims to develop a Protocol on E-Commerce. This has also been formally approved by the African Union Assembly, and it is likely that the timeline for negotiation will be accelerated with the challenges arising from the pandemic.[82] **The AfCFTA could initiate a new, sustainable development approach to rulemaking through PTAs/FTAs, spurring an organisational trade regime ancillary to the WTO, driven by the economic and social developmental considerations of the less legally and economically developed nations in Africa.** The consequence of this is that it will ensure that African nations will have an equal voice in crafting emerging law. Over time, the rules-based approach, and advances in international law, established through the AfCFTA, could shape other trade agreements as well as future rounds of multilateral negotiations.

Although many African countries currently do not have regulations specifically dealing with cross-border data flows, there are differing approaches to digital regulation that appear throughout Africa from the countries that do have such regulation in place. These approaches range from umbrella laws that cover all or most core regulatory areas in the digital space to separate laws for different aspects of digital regulation. Using the AfCFTA as a springboard for PTAs/FTAs, the African Union's Digital Transformation Strategy for Africa addresses transboundary challenges, especially the interoperability of systems, as well as the harmonisation of digital identity systems. The Strategy commits member countries to promote open standards and interoperability to enhance trust in cross-border transactions, personal data protection and privacy.[83]

AU Member States could utilise the AfCFTA to develop a regional cross border data transfer centric trade approach, providing a recognised certification mechanism in a similar form to that of the APEC CBPR System, allowing an automatic display of adequacy for organisations who wish to transfer data amongst the various countries in the African Union. AU Member States could also draw from the principles of "open data" as expressed by the European Commission's regulatory endeavours.[84]

Footnotes

82. African Union, Assembly of the Union, Thirty-Third Ordinary Session, Decision on the AfCFTA, Assembly/AU/Dec. 751 (XXXIII) (Feb. 9-10, 2020).
83. African Union (2019), The Digital Transformation Strategy for Africa (2020- 2030).
84. Ibid footnote 6.

Regional opportunities for Africa: unpacking the solutions continued

The options available to regulators in SADC

Based on the above, regulators have a number of options for shaping their participation in the global digital economy, although the focus of this paper is the SADC region, these option can be further expanded to apply at a pan-African level with adaption to other RECs and national governments:

- **Option 1 – Regional cooperation via policies** – to enable a regional solution for cross-border data flows, the best avenue to implement a sustainable, enforceable and economically viable framework may be leveraging the AfCFTA. Regulators and governments could utilise the expertise of companies operating across different jurisdictions on the African continent, who can work side-by-side with them to create the appropriate framework conditions for business operations, leveraging their experience and technical capabilities to craft policy that accelerates the development of the critical ICT sector. In doing so, the rationale that has been at the forefront of data localisation policies ought to be reconsidered to facilitate the evidenced functionalities that these companies possess. In other words, regulators could work with these companies to craft certification mechanisms for CSPs that can be implemented as a standard at a regional level, which allow CSPs to easily and securely effect cross-border data transfers.
- **Option 2 – Regional cooperation via trade agreements** – to enable the free flow of data across a select few jurisdictions, regulators may be guided by the Australian-Singaporean approach under the DEA or APEC CBPR System. This would involve approaching the respective ministries, regulators and data protection authorities within the relevant jurisdictions across the SADC region to ensure a consensus is reached on appropriate cross-border data flow rules and certification mechanisms. This would be recommended where jurisdictions present incongruence in their respective data protection regulations, standards and in their approach of what would amount to an adequate level of data protection.
- **Option 3 – Regulatory reform** – If regulators or data protection authorities within a particular jurisdiction wish to amend a specific aspect of their data protection or cloud services regulations, particular attention is drawn to jurisdictions that have more enabling data protection legislation already in place, particularly to deal with cross-border data transfers and enabling the use of new technologies, with demonstrable benefits being achieved through same and also, the expressions and significant benefits of 'open data' in jurisdictions such as the EU. SADC Member States are encouraged to accelerate the implementation of core economic integration frameworks and protocols such as the SADC Model Law on Data Protection to reduced regulatory barriers and enable secure and easily facilitated cross-border data flows.

Overall, each SADC country should consider the most appropriate approach to achieving the maximum economic benefit. To this end, one of the above-mentioned approaches or the appropriate combination of policy development and regional cooperation may guide future reforms.

This may include the use and application of TFAs and PTAs as seen in the Australian-Singaporean approach, which would enable the free flow and transfer of data across the countries that are subject to such agreements. The success of these TFAs and PTAs are dependent on the willingness of established data protection authorities to work with their counterparts in foreign jurisdictions to establish independent certifications that will govern the elements, which ensure an adequate level of protection and security. The principles of open data should also be at the forefront of any framework or trade agreement regulating the transfer of data between the SADC or AU member states.

Recommendation for other AU Member States

- AU Member States are encouraged to **implement systems and programmes** to foster the **operationalisation** of AfCFTA, DTS, DPF etc., to realise the full economic and social benefits of cross-border digital and data services.
- There is need for **regulatory reforms** across AU Member States for effective data protection legislation which allows for responsible use of data through digital, cloud or data services, while at the same time providing adequate protection and safeguards for such data use.
- Specifically, AU Member States are encouraged to work with African Union (AU) organs such as the **African Union Development Agency (AUDA-NEPAD)**, the **AfCFTA Secretariat** and the **private sector** to develop and/or amend data protection laws and regulatory frameworks to harness the full potential of data services and digital economies at large.
- AU Member States are recommended to **establish data protection agencies or equivalen**t to address and oversee the 'adequacy requirements' under data protection laws.
- AU Member States can also **learn from the experiences of data flow regulatory frameworks from the ASEAN region and Europe**, e.g., Australian-Singaporean approach under the DEA.
- AU Member States are recommended to **ratify international conventions such as Convention 108+ and create enabling environment** for spawning digital businesses as well attract FDIs into the creation of cloud data centres across the continent.
- Regional Economic Communities ("**REC**"s) are encouraged to implement programmes for the **harmonisation** and **standardisation** of data regulation and legislation across Member States to create the enabling environment for digital businesses.

Applying enabling policy considerations in selected african countries

Democratic Republic of Congo (DRC)

Currently, the DRC does not have a specific data protection law. However, there are regional and sectoral laws that regulate data protection, cybersecurity and cybercrime. A draft law on cybercrime and cybersecurity dealing with the protection of personal data has been submitted to the Parliament on 7 of February 2020. Although the DRC is part of the African Union, it has yet to ratify the African Union Convention on Cyber Security and Personal Data Protection (27 June 2014).

The law of 25 November 2020 relating to telecommunications, information and communication technologies is considered as the only specific law which contains provisions governing data protection and/or cloud computing in the DRC. The law of 25 November 2020 does not provide specific requirements relating to cross-border data transfers or an adequacy requirement for cross-border transfers of personal information but it does provide that an Order from the Minister of Telecommunication would set out the conditions for the transmission of personal data, the publication of which is awaited.

It would be beneficial for the DRC to consider the suggestions set out above while their data protection law is still before Parliament. Separating the requirements for cross-border data transfers across specific industry sectors could lead to a confusing legal regime which could result in a lack of standardisation and inconsistency in practice. The changing nature of the Fourth Industrial Revolution has resulted in many companies adopting a 'one-stop shop' approach to their product offerings. It is not uncommon to see a telecommunication company that also offers mobile money or financial services. If there are numerous laws that each contain their own rules and regulations regarding data protection and cross-border data flows, these companies will be faced with a significant and costly compliance burden, which may result in a negative impact on growth and competition in the country.

Additionally, relying on Ministerial decrees or orders for guidance as to the relevant conditions attached to cross-border data flows allows laws to be updated by a decree as and when new technology becomes readily available and ensures that laws remain modernised in keeping with developments in the ICT sector. However, the creation of a separate data protection authority would be more appropriate. An independent data protection authority would allow the DRC to comply with many of the international model laws and standards that have been adopted over the last few years. The independent data protection authority will also serve as a contact point for foreign counterparts who will require such an authority to both co-operate on FTAs/PTAs and any cross-border criminal and cybercrime investigations. There is therefore a need for harmonization and standardization across AU Member States to create the enabling environment for digital businesses.

Applying enabling policy considerations in selected african countries continued

Mozambique

Many of the same considerations related to the DRC apply to Mozambique. There are no specific laws applicable to cloud and data services or data protection. However, there are specific provisions in the Regulation for the Security of Telecommunication Networks (Decree 66/2019, of 1 August) that refer to operators that use cloud computing to provide their services. **Mozambique is also a recent signatory to the African Union Convention on Cyber Security and Personal Data Protection, having signed on 26 June 2018. Mozambique also ratified the AU Convention in December 2019 and this could indicate a general direction for how a data protection framework may develop in the jurisdiction.**[85]

In the absence of specific legislation permitting the transfer of information outside the borders of Mozambique, companies within Mozambique are required to obtain a judicial authorisation for such cross-border transfer of information. The manner in which such authorisations are obtained remains unclear and therefore a comprehensive and specific data protection regime is preferable. Mozambique should work towards developing a comprehensive and easily accessible data protection law that focuses on the elements of open data and open banking as seen in the EU.

Either signing and implementing Convention 108+ or modelling their law on the provisions thereof would be beneficial to establishing an adequate data protection regime that would be recognised globally. In this regard, **Mozambique could consider adopting expressly defined certification mechanisms within their law to better enable cross-border data transfers and cybersecurity frameworks.**

Tanzania

Tanzania does not currently have specific legislation that comprehensively covers data protection and/or cloud and data services. The Data Protection and Privacy Bill was formulated in 2014 but has not yet been passed into law. There are specific data protection regulations and requirements falling specifically under the banking and finance regulatory framework of the Bank of Tanzania. These regulations do not apply to entities that are not regulated by the Bank of Tanzania.

Whilst there is no specific law governing cross-border data transfers, the Bank of Tanzania has issued a circular (Circular Number FA.56/293/01/54 Circular dated 23 August 2019) requiring all licensed banks and financial institutions (including mobile money operators) to set up either their primary or secondary data centres in Tanzania. Tanzania has also signed and ratified the AU Convention at the end of 2021.

As with Mozambique and the DRC discussed above, the same considerations must be noted while Tanzania engages in the process of implementing a specific data protection law. **As there is a distinct element of data localisation for those regulated by the Bank of Tanzania, Tanzania could also consider ratifying the Convention 108+ and adopting its principles as a basis to develop a suitable data protection regime, which is both cognisant of the downsides associated with data localisation and the benefits of implementing a specified certification mechanism that will enable a standardised and secure means for transferring all types of data across the borders of Tanzania.**

Ethiopia

Ethiopia does not have a single and comprehensive legal instrument regulating privacy and data protection. While rules contained in the Constitution of the Federal Democratic Republic of Ethiopia (1995) and in various specific pieces of legislation which deal directly or indirectly with data privacy and/or data protection and also have application for specific sectors, a Draft Data Protection Proclamation has been issued, which is yet to be approved.

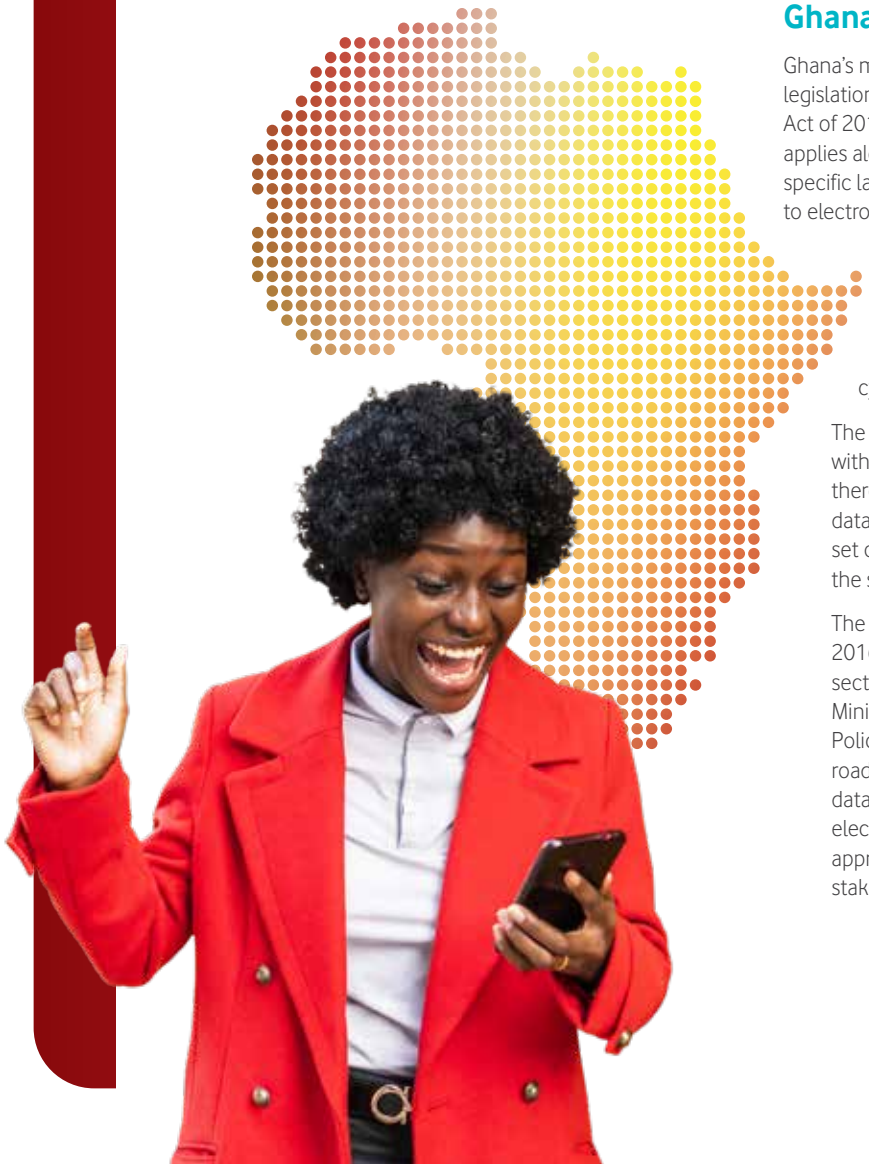
Specifically, cross-border transfers, according to the Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020, prohibits Point of Sale machine operators from sending domestic payment information outside of Ethiopia for authorisation, clearing and settlement. They can only send payment data made through the international card scheme to a bank or microfinance institution licensed by the Bank of Ethiopia. In the same way, Automated Teller Machine operators also may not send any transaction data outside Ethiopia for the purpose of processing, authorisation and switching.

As Ethiopia is also in the process of implementing a specific data protection law, it may benefit from considering the impact of the digital economy on its market and in particular, also look to addressing the elements of data localisation requirements currently in place and consider adopting an appropriate mechanism for allowing cross-border transfers with appropriate safeguards in place in line with Convention 108+ standards and other progressive data protection law models.

Footnotes

85. There are currently 10 countries, including Tanzania and Morocco, which have ratified African Union Convention on Cyber Security and Personal Data Protection, 15 ratifications are required for the convention to come into effect.

Applying enabling policy considerations in selected african countries continued



Ghana

Ghana's main data protection legislation is the Data Protection Act of 2012 (Act 843), which applies along with other sector specific laws (including in relation to electronic communications and financial data). Ghana also has legislation that addresses cloud data transmission and storage via The Electronic Transaction Act, 2008, which also deals with cybercrimes. The Ghanaian parliament has also recently passed the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities in Ghana.

The Ghanaian Data Protection Act does not specifically deal with the cross-border transfer of personal data and therefore this may be carried out with the consent of the data subject or subject to complying with certain conditions set out in the Act. The Act does however specifically prohibit the sale, purchase or reckless disclosure of personal data.

The Banks and Specialised Deposit-Taking Institutions Act, 2016 applies specifically to data in the financial services sector and the Government of Ghana has, through the Ministry of Finance, released a Digital Financial Services Policy. One of the objectives placed on the 2020-2023 roadmap is to introduce a data-sharing regulation between data controllers (banks, mobile network operators, electronic money issuers, social media platforms) and other appropriately regulated Digital Financial Services stakeholders.

With a data protection law already in place aligned to the ECOWAS initiative, Ghana would be well served to ensure that it modernises its existing legislative framework in line with the regional and global changes to ensure it remains in line with developments to adequately support the growth of the digital economy in Ghana.

Lesotho

Lesotho has specific data protection laws in place in the form of the 2011 and 2013 Data Protection Acts.

Chapter 8 of the 2013 Act deals with cross-border data transfers and contains adequacy type provisions for third countries to which personal information is transferred. As with eSwatini, the 2013 Act also caters for exceptions for countries who have enacted a data protection law that contain the provisions of the SADC Model Law on Data Protection making cross-border data transfers from Lesotho to those countries easier.

Summary

The importance of clear and economically considerate regulations relating to cross-border data transfers and cloud services activities is evident. **Regulatory limitations on cross-border data transfers hinder the myriad of benefits to be derived from a digital economy resulting in adverse impact on business opportunities, while also reducing the ability of organisations to trade regionally and internationally, leading to a reduced geographical footprint and reduction in market competitiveness.**

The main barriers hindering scalable data-centric growth in the digital economy are restrictive data localisation requirements, unclear and underutilised adequacy requirements/decisions, and a lack of standardisation as it relates to both policy and legislative terminology.

Data regulations that are purposefully similar in concept, terminology and application with that of other jurisdictions ensure both economically and socially beneficial outcomes for the businesses and individuals of those jurisdictions and allow for more effective regulation by the relevant authorities. Data protection regulation that is considerate of the above ensures the enablement and improvement of trust and trade in the cross-border movement of data. The areas of focus for policy makers highlighted here are interdependent and should be addressed in a way that harmonises laws and policy with the benefits of enabling cross-border data flows. **If market barriers, caused by restrictive and low levels of data protection laws, are addressed enterprises will be able to bring cross-border services to market, making which will allow for new, domestically incorporated SMEs, who do not have the resources of their larger international counterparts, to compete fairly and effectively.** Without improving the interoperability between data protection laws, the friction in making connections between countries and networks will only increase as more enterprises or service providers enter the market.

Without addressing security and trust in cross-border data flows, cyberattacks and fraud will disrupt both enterprises and governments across borders. Consistency in policy and law will ensure that those who perpetrate these cybercrimes are not afforded safe havens from which to conduct such operations. In other words, **globally recognised standards and principles that are expressed in regional frameworks will ensure that opportunistic cybercriminals will have less room to exploit gaps in local cybersecurity and data protection standards.** Enabling cross-border data flows also has the added benefit of allowing the use of AI and machine learning to better understand aspects such as fraud and cybercrime.[86]

As such, data protection laws that enable regional facilitation of cross-border data flows are unified by one key factor, namely, intergovernmental co-ordination and co-operation. We have highlighted the benefits of enabling cloud services through cross-border data flows both from a social and economic perspective. Data protection authorities and governments respectively should have this as a key focus as we venture further into the Fourth Industrial Revolution. Africa has a unique opportunity to start this process as many countries on the continent are still developing or have only recently developed their own data protection laws and regulations with the aim of protecting the individual or business to whom the data relates. This common ground that should form the basis for any negotiation and/or implementation of regional data protection laws, regulations, policies and agreements. Only then may countries in Africa realise the full benefits of a digital economy.

Footnote

86. As an example, according to VISA, the use AI and machine learning allows them to continually improve fraud detection services. In the span of just one year, one of Visa's AI-based technologies allowed them to prevent $25 billion in fraud. According to VISA, this was thanks largely to robust data flows.

References

- Africa in particular has been exhibiting the fastest growth in this regard, with an internet penetration growth rate of 12,441% from 2000 to 2020. Vuleta, Branka. "How Much Data Is Created Every Day? [27 Powerful Stats]." SeedScientific, 28 January 2021, https://seedscientific.com/how-much-data-is-created-every-day/
- African Union (2019), The Digital Transformation Strategy for Africa (2020- 2030).
- African Union, Assembly of the Union, Thirty-Third Ordinary Session, Decision on the AfCFTA,
- Agreement Establishing the African Continental Free Trade Area
- Anne Josephine Flanagan, Nada AlSaeed, Lothar Determann and Leanne Kemp "A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy" World Economic Forum White Paper (2020).
- APEC (2005) APEC Privacy Framework, available at https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdfAsyraf Kamil "'Hundreds of jobs' available at Facebook's S$1.4 billion facility in Singapore slated to open in 2022" (2018)
- Chander, Anupam, and Uyên P. Lê. "Data nationalism" Emory LJ 64 (2014) 677.
- Cisco, "The Zettabyte Era: Trends and Analysis," White paper (2017)
- Cisco Annual Internet Report (2018–2023), White paper (2020) available at https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data
- Congressional Research Service. "The North American Free Trade Agreement ('NAFTA')".
- Data from the Bank of Mauritius indicate that Mauritius' total foreign direct investment inflows amounted to 21,337 million Rupees in 2019 – Bank of Mauritius, "Preliminary Gross Direct Investment Flows: 2019" (Excluding Global Business Sector)
- EC, Final report of the High Level Forum on the Capital Markets Union: A new vision for Europe's capital markets (2020), Recommendation on Cloud, pg.82–84.
- ECPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in EU Member States (2016).
- European Commission, "A European Strategy for Data" COM (2020) 66, found here.
- Expert Group on Regulatory Obstacles to Financial Innovation, 30 Recommendations on Regulation, Innovation and Finance: Final Report to the European Commission (2019).
- Full List of Convention 108 Signatories
- G. Greenleaf 'Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives' (2016) 142 Privacy Laws & Business International
- Gurumurthy, Anita, Amrita Vasudevan, and Nandini Chami. "The Grand Myth of Cross-Border Data Flows in Trade Deals" IT for Change (2017).
- Hosuk Lee-Makiyama, Badri Narayanan and Simon Lacey, "Cross-Border Data Flows The impact of data localisation on IoT" GSMA, January 2021, https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf (accessed 15 July 2022).
- Indian Council For Research On International Economic Relations, "Regulatory Burden on Micro-Small and Medium Business due to Data Localisation Policies" *Data Catalyst* (2019).
- James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra, "Digital Globalization: The New Era of Global Flows" *McKinsey Global Institute*, (February 2016), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.
- Julius Nyamwena and Pamela Mondliwa, "Policy Brief 3: Data Governance Matters: Lessons For South Africa", *The Industrial Development Think Tank* (2020).
- Lawfare, "Cross-border Privacy Rules in Asia: An Overview," (2019) available at https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview
- Mark Beech, "COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal," Forbes (2020) available at https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=313ce78d3104
- Meltzer, J. P. (2015), "A New Digital Trade Agenda", E15 Initiative. https://e15initiative.org/publications/a-new-digital-trade-agenda/
- Ministry of Trade and Industry Singapore Digital Economy Agreements (mti.gov.sg).
- Pepper, R., Garrity, J., and LaSalle, "Cross-Border Data Flows, Digital Innovation, and Economic Growth." *In The Global Information Technology Report 2016 – Innovating in the Digital Economy*, edited by Silja Baller, Soumitra Dutta and Bruno Lanvin, 39-47. Cologny: World Economic Forum

References

- Read the Belgian DPA approval decision regarding EU Cloud Code of Conduct, the accreditation decision regarding Scope Europe and the Belgian DPA's press release regarding the approval decision.
- Reportlinker.com "Data Center Market in Africa – Industry Outlook and Forecast 2021-2026" (2021) available at https://www.reportlinker.com/p05822887/Data-Center-Market-in-Africa-Industry-Outlook-and-Forecast.html?utm_source=GNW .
- Samuel Stolton, " What's behind the EU's new Cloud Code of Conduct?" 25 May 2021, IAPP available at https://iapp.org/news/a/whats-behind-the-eus-new-cloud-code-of-conduct/
- Sharma, Aprajita. "Data Localisation May Hit GDP, Ease of Doing Business Ranking, Says Report." *Business Today*, 20 November 2018, https://www.businesstoday.in/current/economy-politics/data-localisation-may-hit-gdp-ease-of-doing-business-ranking-says-areport/story/292799.html.
- Template contract clause for transfers of data to overseas recipients that hold CBPR certifications can be found here
- The Australian Office of the Australian Information Commissioner and the Singaporean Personal Data Protection Commission's Memorandum of Understanding.
- Turco, K., 2021. Top 4 Advantages of Software as a Service (SaaS) | TechnologyAdvice. Available at: https://technologyadvice.com/blog/information-technology/advantages-of-software-as-a-service-saas-2/(Accessed 15 July 2021).
- Ubaldi "Governments In: State of Open Data. Open data for development" (2019)
- UN General Assembly, seventy-third session *Report of the Special Rapporteur on the right to privacy*, 17 October 2018, http://www.worldlii.org/int/other/UNSRPPub/2018/11.html
- Unctad.org. 2019. *Young digital entrepreneurs leading Africa into a new era* | UNCTAD. Available at: https://unctad.org/news/young-digital-entrepreneurs-leading-africa-new-era (Accessed 15 July 2021).
- VISA, the use AI and machine learning allows them to continually improve fraud detection services. In the span of just one year, one of Visa's AI-based technologies allowed them to prevent $25 billion in fraud. According to VISA, this was thanks largely to robust data flows.
- "Volume of data/information created worldwide from 2005 to 2025 (in zettabytes) available at https://www.statista.com/statistics/871513/worldwide-data-created/,"
- What is PaaS? Platform as a Service | Microsoft Azure. Available at: https://azure.microsoft.com/en-us/overview/what-is-paas/ (Accessed 15 July 2021).
- Wu, M. (2017), Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System, RTA Exchange, Geneva: ICTSD and the IDB, available at http://e15initiative.org/publications/digital-trade-related-provisions-in-regional-trade-agreements-existing-models-and-lessons-for-the-multilateral-trade-system/

Further together