AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, Ethiopia P. O. Box 3243 Telephone: 5517 700 Fax: 5517844
Website: www.au.int

EXECUTIVE COUNCIL
Fortieth Ordinary Session
20 January - 03 February 2022
Addis Ababa, Ethiopia

EX.CL/1308(XL)
Original : English

REPORT OF THE 4TH ORDINARY SESSION OF THE STC ON COMMUNICATION AND ICT (STC-CICT), 25-27 OCTOBER 2021

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

FOURTH ORDINARY SESSION OF THE AFRICAN UNION SPECIALIZED TECHNICALCOMMITTEE ON COMMUNICATION AND ICT (CCITC-4), BY VIDEO CONFERENCE, 25-27 OCTOBER 2021

MINISTERIAL SESSION

27 October 2021

MEETING REPORT

INTRODUCTION

1. The Fourth Ordinary Session of the African Union Specialized Technical Committee (STC) on Communication and ICT (CCICT) was held by video conferencing on 27 October 2021. The meeting was preceded by experts' sessions held from 25 to 26 October 2021

ATTENDANCE

2. The following 37 Member States took part in the meeting: Algeria, Angola, Botswana, Burkina Faso, Burundi, Cameroon, Chad, Central African Republic, Comoros, Congo (Democratic Republic), Congo (Republic), Côte d'Ivoire, Djibouti, Egypt, Equatorial Guinee, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Kenya, Lesotho, Libya, Morocco, Mozambique, Namibia, Niger, Rwanda, Sahrawi Arab Democratic Republic, Senegal, South Africa, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe. The list of participants is attached as **Annex I**:

3. AUDA/NEPAD and the following Regional Economic Communities (RECs) were also in attendance: Economic Community of Central African States (ECCAS).

4. The following African and International Organizations and Agencies also took part: African Telecommunication Union (ATU), Pan African Postal Union (PAPU) and Smart Africa.

5. The following organizations were also present: International Telecommunication Union (ITU), European Union (EU), World Bank (WB), GIZ, Internet Society (ISOC), Huawei and ICT Research Africa.

I. OPENING CEREMONY

6. The ceremony was skipped to focus on getting the required quorum for the meeting to proceed.

II. ELECTION OF CCICT-4

7. Based on the principle of rotation and geographical representation, the following Bureau of the STC-CICT-4 was elected.

AFRICA	
Congo (Rep)	Chair of the Bureau
AFRICA	
South Africa	1st Vice Chair of the Bureau

AFRICA	
Niger	2nd Vice Chair of the Bureau
AFRICA	
Rwanda	3rd Vice Chair of the Bureau
AFRICA	
Egypt	Acting Rapporteur of the Bureau

8. Northern Africa will consult and confirm the Member State to be designated as Rapporteur in due course.

III. AOPTION OF AGENDA AND WORK PROGRAM

9. The meeting adopted the following agenda with amendment with amendments.

1) Opening ceremony
2) Election of the Bureau;
3) Adoption of agenda and work program;
4) Report of the experts' report;
5) Consideration and adoption of the 2021 Declaration
6) Consideration of draft continental frameworks on digital id interoperability and continental data policy;
7) Consideration and adoption of ministerial report;
8) Any other business.
9) Closing ceremony.

10. The adopted work programme is attached as **Annex II**.

IV. CONSIDERATION OF THE REPORT OF EXPERTS.

11. The Acting Rapporteur, Egypt, presented the report of experts. The report highlighted achievements and challenges occurred and comments made by the experts as follows.

AU Commission

- Digital Transformation Strategy (DTS) for Africa with the development of AU Digital Health Strategy and Implementation plan, AU Digital Education Strategy and Implementation Plan, AU Digital Agriculture Strategy and Implementation plan, AU E-Commerce Strategy, Guidelines on common approach on postal digital transformation in Africa and development of M&E Framework for the Digital Transformation Strategy for Africa (DTS);

- Draft AU Interoperability Framework for Digital ID and AU Continental Data Policy Framework;

- Second phase (2021-2030) of PIDA that includes projects on ICT along with Water, Energy and Transport, a total of 69 / 12 projects on ICT were selected and validated by the AU summit in February 2021 to reinforce intra-Africa connectivity and is based on the integrated corridor approach that seeks to leverage digital technologies for the development of smart infrastructure.

- Policy and Regulation Initiative for Digital Africa (PRIDA) with notably the selection of Conditions of Entry into the Market (Authorization/Licensing Regime) and Protection of Personal Data and Data Location as topics for harmonization of indicators and Monitoring and Evaluation (M&E) Methodology on the two topics and the development of two M&E Prototypes to measure the extent of harmonization of each topic across the continent.

- Cybersecurity highlighting progress made in reviewing of the Malabo Convention and the development of a Continental Child Online Safety Policy and a Continental Cybersecurity Strategy;

- AU Policy recommendations on Digital Solutions to Trace, Diagnose and Share Information about Pandemics in Africa.

- Building the AU Brand Identity and Promoting AU Mandate and Agenda marked by institution of the new brand identity across the AUC and AU Organs, promotion of Agenda 2063 on both traditional media and digital platforms to improve awareness and knowledge of Agenda 2063 as well as understanding of AU Mandates and Programmes;

- Improving Corporate Visibility, Advocacy and Public Relations highlighting development and launching of 2 mobile applications to reach mobile phone and tablet users, advocacy initiatives to ratify the AU treaties, holding of Annual African Women in Media and re-prioritisation of activities towards positioning the African Union and Africa CDC on the forefront of managing and combatting the Covid-19 pandemic in Africa.

AUDA Nepad

- In line with the Malabo Convention on Cybersecurity and Personal Data Protection, AUDA-NEPAD undertook cybersecurity assessments in ten African Union member states - Benin, Chad, Republic of Congo, Democratic Republic of Congo, Guinea, Kenya, Mauritania, Morocco, Senegal and Tunisia and published individual country reports as well as a

consolidated report – AUDA-NEPAD Cybersecurity Assessment Report (https://www.au-pida.org/download/cybersecurity-assessment-report/).

- AUDA-NEPAD is also collaborating with the Global Forum on Cyber Expertise (GFCE) on a project which aims to develop Cyber Capacity Building (CCB) knowledge to enable AU Member States to better understand cyber capacities as well as identify and address their national cyber capacity needs and also strengthen their cyber resilience.

- The second PIDA Priority Action Plan (PIDA PAP II) was adopted by the AU Assembly in February 2021. Of the 69 projects, 11 are in the ICT sector.

PAPU

- Progress made in the implementation of the project on connectivity and Electrification and connectivity of Post Offices in rural areas Kenya, Malawi, Tanzania and Uganda that have shown remarkable progress in the mobilisation of funds and implementation of the project.

- PAPU and Member States implemented strategies to fight against COVID-19 including deepening of remittances and e-Services offered. is concerned, The following, among others, additional measures were put in place:

- PAPU advised member countries to issue EmiS (Emergency Information system messages) on the effects of COVID-19, best practices to be adopted during the pandemic period as well as how the post can remain relevant;

- PAPU circulated a questionnaire in April, 2020 to assess the situation in Member States and how they were coping under the circumstances;

- Held a webinar with AFRAA on 12th May, 2020, and concluded that the post offers essential services and that governments should therefore be sensitized as such to facilitate the movement of mail using cargo planes.

ATU

- Preparation for ITU World Radiocommunication Conference (WRC-23), Standardization Assembly 2020 (WTSA-20), World Telecommunications Development Conference 2021 (WTDC-21) African Preparatory meetings for ITU PP-22

STUDIES UNDETAKEN & REPORTS DEVELOPED BY ATU

(a) **4IR Strategy:** with the support of the Government of South Africa recruited a Consultant Cabinet and develop the draft of the 4th industrial (4IR) Strategy that was presented to ATU Members for the first time in October 2020 during a validation Workshop and then reviewed taking in account Members inputs and comments and submitted to the ATU Council session 2021.

(b) **E-Waste Management:** ATU also developed guidelines on E-waste management for Africa and ATU is liaising with membership on the implementation of these guidelines. ATU looks forward to collaborating more with AUC in supporting this process as we all strive to serve the continent.

(c) **Digital innovation Challenge:** ATU also successfully conducted 2 editions of the 'ATU Africa Innovation Challenge 2020 & 2021 in collaboration with ITU and other partners with the objective to promote the innovation spirit in Africa and provide an unique opportunity to young Africans to express their innovative ideas and talent and recognize the important role of the ecosystem the achieve the digital development in Africa. This year 2021's edition of the Challenge identified institutions from Africa that create an enabling environment for youth to develop ICT innovations. Among the institutions sort to take part in the competition included policy making bodies, incubators, universities and non-profits. This is in recognition of the critical role that such organizations play and the importance of investing in fertile soil from which innovators can grow from. The Challenge culminated in an award ceremony held in October 2021 where the top 10 winners were awarded with cash prices and attributed the title of "2021 ATU Best Ecosystem Practice in Africa Enabling Youth ICT Innovation".

(d) **Migration to IPv6 strategy:** ATU also developed an IPv6 Migration strategy framework for Africa and in partnership with Afrinic, ATU aims to develop a capacity building programme in this regard and looks forward in liaise with its membership and stakeholders to the implement the strategy in collaboration with AUC and sister organizations in supporting this process as we all strive to serve the continent.

(e) **E-skilling Model framework:** ATU also developed an e-skilling model framework for Africa to address the future needs of the Africa digital market and looks forward in liaise with its membership, partners and stakeholders to the implement this model in collaboration with AUC and sister organizations in supporting this process as we all strive to serve the continent. The ATU ICT day to be held on 7th

December 2021 will be celebrated under the theme: "Digital Skills Development for Africa's Digital Transformation".

ONGOING OR RECENTLY COMPLETED PROGRAMS

- **Radio communication**

(a) Development of recommendations on the implementation of emerging technologies aimed at guiding African countries on implementing these emerging technologies including 5G;
(b) Development of recommendations aimed at guiding African countries on modern spectrum management practices;
(c) Optimization of the FM Broadcasting Frequency Plan (the GE84 Plan) for Africa aimed at identifying new usable channels to sustain the growth of FM radio in Africa;
(d) Development of a Strategy for introduction of digital sound broadcasting in Africa;
(e) The 1st edition of the African Spectrum Plan (AfriSAP) aimed at being the reference for sub-regional and/or national spectrum plans has been developed;
(f) Harmonization of Frequencies for Emergency Telecommunications (PPDR) has been completed alongside the said AfriSAP;
(g) Development of a strategy for satellite orbital and frequency resources management aimed at optimizing the acquisition, retention and use of these resources in Africa has been developed;
(h) Development of recommendations aimed at guiding African countries on how spectrum policy, regulations and practices can foster rural connectivity.

- **Standardization & Development sectors**

(a) Development of a model framework/guidelines on Data Centers and Cloud Computing services and Infrastructures for Africa;
(b) Development of a white paper on connectivity and accessibility best practices in Africa and a regional framework to facilitate access to submarine cables to all countries particularly land locked countries.
(c) Development of a common digital security policy and standards for network security and information systems;
(d) Capacity building in partnership with Huawei on emerging technologies and digital tools (cloud computing, etc...);

(e) White paper on access and connectivity and Cooperation framework to facilitate access to submarine FO cables for landlocked countries;
(f) Study to develop an ICT Observatory for Africa.

12. Challenges raised include:

(i) limited Resources to implement the Digital Transformation Strategy for Africa and lack of framework and mechanism for monitoring and evaluating implementation of the strategy,
(ii) travel restrictions arising out of the COVID-19 pandemic and Closure of government offices due to COVID-19 (a challenge where information online is limited),
(iii) Few digital economy policies at Member State and Regional levels that facilitates an enabling digital trade and digital economy environment,
(iv) limited participation on data sharing or collection, weak resource mobilization for PIDA projects preparation particularly the domestic resources,
(v) delays in PIDA agreements between countries and non-alignment for legal and regulatory framework for concerned countries and appointment of PIDA sectorial focal persons from some Member States/Ministries,
(vi) Insufficient budget and understaffing of communication directorate.
(vii) inadequate funding for financing projects such as Addressing and Post Codes, Electrification and Connectivity Project.
(viii) Procurement of digital solutions for postal financial services, especially in the wake of the Covid-19 Pandemic and
(ix) High conveyance rates due to use of cargo rates for mail conveyance instead of using the lower UPU/IATA mail rates.
(x) Deployment of strategies to fight against COVID-19 including deepening of remittances and e-Services offered.

13. The report is attached as **Annex III.**

14. The ministers took note of the report and made following comments:

(i) Commend to the experts for the work done in this trying time;
(ii) Request to mention that Egypt is Ag Rapporteur as the Northern region with pursue consultation to agree on the country to be designated.

V. Consideration of AU Interoperability Framework for Digital ID and AU Continental Data Policy Framework

15. Following presentation of the two frameworks, the ministers made the following recommendations:

AU Interoperability Framework for Digital ID

(i) Member States to provide input within 1 month to the draft AU Interoperability Framework for Digital ID to enable its adoption by AU Policy Organs
(ii) Commend the AUC on the excellent work done;

AU Continental Data Policy Framework

(i) Member States to provide input within 1 month to the Draft Continental Data Policy Framework to enable its adoption by AU Policy Organs.

(ii) Commend the AUC on the excellent work done.

VI. Consideration and adoption of the 2021 declaration (Annex IV).

16. The declaration was adopted with amendments.

VII. Consideration of date and venue of the next STC

17. The Republic of Congo offered to host the 5th Ordinary session of the STC in 2023.

18. In collaboration with the Bureau of the STC and the AU Commission the date of the STC will be set in due course.

VIII. Consideration and adoption of ministerial report

19. The AU Commission was requested to circulate the report among Member States.

IX. Any Other Business

20. None

X. Closure of the meeting

21. In her closing remarks, H.E. Dr Amani ABOU-ZEID, AU Commissioner for Infrastructure and Energy, African Union Commission thanked the Chairperson of the outgoing Bureau of the STC on Communication and ICT for his leadership in steering the work of the STC over the period 2019-2021 and congratulated him for the achievement in the two sectors despite the challenge caused by the on-going COVID-19 pandemic.

22. She also gave a warm welcome to the new Chair of the STC on Communication and ICT and the elected Bureau and reassure them that together with my team we will be working with the Bureau tirelessly to enhance Africa's Digital Transformation.

23. She concluded by assuring the Ministers that the African Union Commission will continue building of stronger partnerships and collaborations and work with all stakeholders to harness technology for the good, and ensure that it is inclusive and safe and deploy it to increase the momentum of the Covid-19 recovery.

24. On his side, H.E. Minister Léon Juste IBOUMBO, Minister of Posts, Telecommunications and Digital Economy of the Republic of Congo, elected Chair of the Bureau congratulated the ministers and other participants for their commitment and active participation despite the difficult context.

25. The Chair expressed gratitude of the Republic of Congo to his peers specially the ministers from the ECCAS region for its election as Chair of the Bureau as this confirms the pertinence of the vision of the Republic of Congo on digitalization.

26. Mr IBOMBO acknowledged the achievements of the Bureau chaired by Egypt and expressed his wish to benefit from the valuable experience from the members of the outgoing Bureau.

27. Before concluding his speech, the Minister informed the participants about the operationalization by his country of the African Center of Research on Artificial Intelligence and stressed on his readiness to receive all Africans.

FOURTH ORDINARY SESSION OF THE SPECIALIZED TECHNICAL COMMITTEE ON COMMUNICATION AND ICT (CCICT)

27 OCTOBER 2021 THROUGH VIDEO CONFERENCE

AU/STC-CICT-4/MIN/Decl.
ORIGINAL: ENGLISH

2021 STC-CICT DECLARATION

PREAMBLE

WE, the Ministers in charge of Communication and ICT, meeting through Video conferencing on 27October 2021 in the Fourth Ordinary Session of **the Specialized Technical Committee on Communication and ICT**;

GUIDED BY the Constitutive Act of the African Union (AU);

RECALLING Decisions Assembly/AU/Dec.227 (XII) and Assembly/AU/Dec.365(XIVI), adopted in January 2009 and July 2011, respectively, on the configuration of the Specialized Technical Committees (STCs) and the modalities for their operationalization;

BEARING IN MIND Declaration Assembly/AU/Decl.1(XIV), adopted at the 14th Ordinary Session of the Assembly of the AU on Information and Communication Technologies in Africa, Challenges and Prospects for Development, held in Addis Ababa, Ethiopia, in February 2010;

CONSIDERING Declaration Assembly/AU/Decl.2(XVIII), at the 18th Ordinary Session of the Assembly of the AU, held in Addis Ababa, Ethiopia, in January 2012, on the Programme for Infrastructure Development in Africa (PIDA) and Decision Assembly/AU/Dec.529(XXIII) of the 23rd Ordinary Session of the Assembly of the AU held in Malabo, Equatorial Guinea in June 2014 which adopted the African Union Convention on Cyberspace Security and Protection of Personal Data;

CONSIDERING ALSO Declaration Assembly/AU/Decl.3(XXX) adopted at the 30th Ordinary Session of the AU Assembly in Addis Ababa, Ethiopia, held from 28 to 29 January 2018 on Internet Governance and Development of Africa's Digital Economy;

RECALLING the Executive Council Decision EX.CL/1074(XXXVI) on the reports of the Specialized Technical Committees, including the 3rd Ordinary Session of the STC on Communication and ICT, held in Sharm El Sheikh, Arab Republic of Egypt from 25 to 26 October 2019 that endorsed the Digital Transformation Strategy for Africa (DTS) to harness digital technologies and innovation to transform African societies and economies and requested the Commission to undertake the following among others:

(i) Mobilize the necessary resources to implement the Comprehensive Digital Transformation Strategy for Africa and develop the matrix for the implementation of the Strategy;
(ii) Promote the strategy at all AU relevant activities including the STCs;
(iii) Develop sectoral implementation strategies/plans of the DTS including those critical ones already identified to have comprehensive DTS for the continent;
(iv) Develop guidelines on Privacy, Over The Top services (OTT), a continental framework on data policy and a road map and guidelines for spectrum harmonization and deployment for current and future mobile and wireless broadband networks such as International Mobile Telecommunications (IMT) 2020 /5G;
(v) Dedicate appropriate resources for the implementation of a comprehensive Cybersecurity program which includes assistance to the

AU Member States to adopt cyber strategies, Cyber legislation and establishment of CIRTs/CERTs;

(vi) Submit a report on Audit of the common assets of the Pan African e-Network with financial implications before applying the recommendation of the relevant Ministers to transfer its assets to RASCOM; and,

(vii) Ensure that the Brand and Communication Style Guide and the Communication Policies and Procedures are instituted within the Organization.

TAKING INTO ACCOUNT the advent of the COVID-19 pandemic and the Communication and ICT sector's response to the pandemic as outlined in the Declaration of the Bureau of the STC-CICT meeting on 5th May 2020;

ACKNOWLEDGING the efforts made by the AUC, AU Specialized Agencies and Regional Organizations as well as international organizations at facilitating and implementing the Digital Transformation Strategy for Africa (DTS) across the continent and in developing sectorial digital strategies for Education, Health, Agriculture, e-Commerce and Postal Sector, drafting AU Continental Data Policy Framework and Interoperability Framework for Digital ID, continental cyber security strategy, child online protection policy paper, Harmonization methodology and template aimed at collecting ongoing and completed projects related to digital transformation in Member States and RECs to improve coordination and facilitate synergies

BEARING IN MIND the unprecedented demand for digital technologies to facilitate containment of the COVID-19 pandemic and applauding the various initiatives to curtail the spread of the COVID-19 as well as mitigate its societal and economic effects;

RECALLING the vision of the Digital Transformation Strategy for Africa to have an integrated and inclusive digital society and economy in Africa that improves the quality of life of Africa's citizens, strengthens the existing economic sector, enables its diversification and development, and ensures continental ownership with Africa as a producer and not only a consumer in the global economy;

ALSO RECALLING the commitment to continue the implementation of the AU communication and advocacy strategy, improve corporate visibility, and build the AU brand under Agenda 2063;

FURTHER RECALLING the Solemn Declaration on the 50th Anniversary of the OAU/AU of May 2013 wherein Heads of State and Government declared their commitment to fly the AU flag and sing the AU anthem along with our national flags and anthems; and to promote and harmonize the teaching of African history, values and Pan Africanism in all our schools and educational institutions as part of advancing our African identity and Renaissance;

BEARING IN MIND the importance of communication, branding, advocacy and public relations to the reputation, recognition and appreciation of the African Union among all its stakeholders;

AWARE OF THE NEED to celebrate the 20th anniversary of the African Union in 2022 continentally and the need to raise the brand of the AU throughout all African populations in the context of the spread of COVID-19;

CONSIDERING the Report of the Experts' Session held virtually, from 25 to 26 October 2021;

HAVING ELECTED the following Bureau of the STC-CICT for a period two (2) years:

CENTRAL AFRICA	
Congo (**Rep**)	Chair
SOUTHERN AFRICA	
South Africa	1st Vice Chair
WESTERN AFRICA	
Niger	2nd Vice Chair
EASTERN AFRICA	
Rwanda	3rd Vice Chair
NORTHERN AFRICA	
TBC	Rapporteur

TAKE NOTE OF the report of the Bureau and **COMMEND** the Bureau for the achievements;

COMMEND ALSO the AU Commission for developing breakthrough policies and forward looking continental frameworks for Digital ID Interoperability and Data Policy that are in line with global best practices.

FURTHER TAKE NOTE the progress made to accelerate implementation of the Digital Transformation Strategy in critical sectors, notably the development of the AU Digital Health Strategy and Implementation Plan, AU Digital Education Strategy and Implementation Plan, AU Digital Agriculture Strategy and Implementation Plan, AU E-Commerce Strategy, Data Policy Framework for Africa, AU Interoperability Framework for Digital ID, initiative to review the AU Convention on Cybersecurity and Personal Data Protection ("Malabo Convention") to conform to latest global standards and norms in cyberspace; initiative to develop the Continental Cybersecurity Strategy and an African Union Child Online Safety and Empowerment Policy, the M&E Methodology and Tool to measure the extent of harmonization of ICT & Digital policies and regulations, and Building the Brand Identity of the AU and working towards creating an enabling environment to facilitate establishment of Africa's Digital Single Market in line with the AfCFTA as well as the work it has done to build the Brand Identity of the AU;

HEREBY COMMIT OURSELVES TO:

1. **CONTRIBUTE** to the coordinated continental response to the COVID-19 pandemic and mitigate its negative impacts;

2. **CONTINUE** developing policies and regulations to facilitate deployment and use of safe and secure digital tools to improve COVID-19 responses;

3. **PROVIDE** feedback within one month to enrich the Draft AU Interoperability Framework for Digital ID and Draft AU Continental Data Policy Framework to enable adoption of the two frameworks by AU Policy Organs;

4. **MOBILIZE** the necessary resources to implement the AU Continental Data Policy Framework;

5. **TAKE NOTE** of the Outcomes of the Audit Report of the Common Asset of Pan African e-Network (PAeN) for Telemedicine and Tele-education as well as the initiative to redesign the Network to deliver up- to date e-education and e-health services.

6. **REAFFIRM** the recognition of posts as important national infrastructure for digital, social, financial and trade's inclusion as well as physical network which complements people's digital needs – link physical to digital worlds;

7. **PURSUE** the policy and regulatory reforms of the postal sector at national, regional and continental levels and facilitate increased investment in digital infrastructure and strengthen the pace of its digital transformation.

HEREBY REQUEST MEMBER STATES TO:

8. **PUT** in place and support the adoption of adequate policies and regulations that facilitate the deployment and use of digital tools and solutions to enable cross sector and interoperability of data to improve COVID-19 responses;

9. **PROMOTE** zero-rating of access to health and educational content as a critical and urgent intervention, to counter the pandemic and to support learners and students confined to home due to the closure of schools, colleges and universities;

10. **USE** digital Platforms, Portals and Applications especially those developed by Africans for Africans, that can help Trace, Track and Test people who have come into contact with an infected person while balancing health imperatives, privacy concerns and data protection;

11. **BUILD** partnerships with private technology companies, social entrepreneurs, national and international organizations to make use of existing technologies to manage the COVID-19 crisis;

12. **ENCOURAGE** the design of new applications and services to help in the fight against COVID-19, to facilitate services such as delivering food and other essential items to those most in need by optimizing the entire supply chain via digital government services;

13. **ENCOURAGE** the sharing of best practices on the digitalization of their postal sector to enable the AUC to finalize and disseminate the Guidelines on Common Approach for digital postal transformation by 31 December 2021;

14. **ENHANCE** capacity building programmes on ICTs and cybersecurity in the

continent and **CONNECT** the unconnected to close the digital divide gap and ensure that all citizens benefit from the use of innovative digital technology solutions to have access to basic services online;

15. **CONNECT** and involve post offices in the implementation of strategies to fight against COVID-19 including widening provision of remittance and e-Services;

16. **PROMOTE** the implementation of the AU Brand & Communication Style Guide and the Communication Policies and Procedures and ensure adoption and use of the AU brand in all Member States;

17. **COOPERATE** with the AUC in making their national public broadcasters available to disseminate information coming from the Commission in the month of September 2022 and May 2023, when the continent will be celebrating the 20th anniversary of the AUC and the 60th anniversary of the OAU respectively. This will be done in the context of ensuring that all African citizens know more about the celebrations and the role of the AU, in the context of building the corporate identity of the AU;

18. **PROMOTE** engagement with Ministries of Education within the Member States to encourage adoption of teaching and dissemination of continental symbols such as the AU Anthem and promote inclusion of Agenda 2063 in national curricula;

19. **ENCOURAGE THE DIGITALIZATION OF INTEROPERABLE HARMONIZED** health credentials that comply with the PANABIOS[1] trusted travel requirements to ensure continued mobility of African citizens within the continent for increased intra-African trade to facilitate implementation of the AfCFTA;

20. **SUPPORT and FACILITATE** the continental implementation of the M&E Models on harmonization of Market Entry Conditions and Data Protection legal and regulatory frameworks;

21. **ENCOURAGE THE USE of** the Harmonization Methodology and Tool to measure the extent of harmonization of ICT & Digital policy, legal and regulatory frameworks both at regional and continental levels;

22. **STRENGTHEN** regulatory cooperation at continental level to collectively respond to the new challenges arising from digitalization and the increasing convergence of services;

23. **ACCELERATE** the implementation of the PIDA-PAP2 project on ICT and advocate for the integration of Digital Technologies in the development of smart infrastructure;

24. **DEVELOP** two pilot projects along main PIDA corridors and into remote areas

[1] PanaBIOS is built by African technologists and AI thinkers to provide biosurveillance and bioscreening technology, data, and insights to enable the creation of Public Health Corridors within the broader AU Open Corridors Initiative.

in line with the AU Strategy for Unlocking Access to Basic Infrastructure and Services for Rural and Remote Areas;

25. **SET UP** multi-institutional working groups on digital ID and data policy at national level.

26. **DOMESTICATE** the AU Interoperability Framework for Digital ID and AU Continental Data Policy Framework, upon their adoption, and establish multi-stakeholder buy-in to enable effective and responsible data circulation and use at national level.

27. **FURTHER REQUEST MEMBER STATES AND RECs** to expedite the development of national policies, agendas, and frameworks on digital economy and digital trade, and intensify cooperation and private stakeholder engagement and dialogues to develop common standards that will in the future act as the foundation of the harmonization of frameworks towards integration of digital economies within the continent.

DIRECT THE AU COMMISSION TO:

28. **RE-CIRCULATE** the draft Digital ID interoperability Framework and Continental data policy framework to Member States for final inputs and finalize the documents to enable their adoption by AU Policy Organs.

29. **PURSUE** the development of the following digital strategies, policy frameworks and projects:

    (i) AU Digital Education Strategy and Implementation Plan, AU Digital Education and Implementation Plan AU Digital Agriculture Strategy and Implementation plan, E-commerce strategy
    (ii) Continental Cybersecurity Strategy;
    (iii) Continental Child Online Safety and Empowerment Policy;
    (iv) Revision of the Malabo Convention on Cybersecurity and Personal Data Protection and expedite the entry into force
    (v) Digital Transformation of the Postal Sector in Africa;
    (vi) Continental Strategy to enhance Harmonization of Digital Policy, Legal and Regulatory Frameworks to support the establishment of Africa's Digital Single Market;
    (vii) Mapping of the digital projects or activities to DTS proposed actions;
    (viii) DTS Implementation Architecture and M&E Framework;
    (ix) Re-design of the Pan African e-Network to deliver e-health and e-education services;
    (x) Continental AI strategy
    (xi) Statistics on digital connectivity and Digital readiness of African countries

30. **WORK** with regional institutions and relevant stakeholders to develop an Action Plan to guide the implementation of the AU Continental Data Policy framework (short, medium and long- term) upon its adoption, including immediate actions to achieve the same level of data readiness at continental level

31. **COORDINATE** the development of a Common Data Categorization Framework and Cross Border Data Flows Mechanism that take into account the broad types of data , their different levels of privacy and security as well as the different levels of data maturity and digital readiness of African countries.

32. **CONSIDER** alignments of the AU Continental Data Policy framework, upon its adoption, with the AfCFTA process by including provisions on data in the negotiations of the competition and intellectual property chapters.

33. **ENSURE** that the Brand & Communication Style Guide and the Communication Policies and Procedures are instituted within the organization and the organs and institutions of the African Union;

34. **UNDERTAKE** a benchmarking exercise of communication budget allocations for institutions of a similar nature and size as the African Union to establish a baseline for communication budget to be used as a guide on recommendation for adequate funding;

35. **ALLOCATE** realistic financial resources to capacitate the information and Communication Directorate (ICD) to enable it to better and effectively communicate to various stakeholders and audiences on different media platforms in a strategic and consistent manner;

36. **PRIORITIZE** the capacitation of the Information and Communication Directorate in the first phase of the Institutional Reforms;

37. **IMPLEMENT** Executive Council Decision EX.CL/Dec.1069 (XXXV) of July 2019 that all AU activities relating to communications shall be managed by the of Information and Communication Directorate;

38. **APPROVE** initiatives aimed at inundating the continent and reaching Africans through the use of national broadcasters to undertake the following activities for the month of September 2022 in commemoration of the 20th anniversary of the African Union:

    (i) Playing the AU anthem on all national broadcast stations at the beginning and end of the day;
    (ii) Raising the AU flag alongside national flags in Member States,
    (iii) Playing a celebratory video to be produced by the ICD on all the TV stations of AU Member States; this video will highlight the road Africa has travelled under the AU, as well as the successes, challenges and mitigatory measures;
    (iv) Broadcast on national TV and radio stations an online social media conversation with Africa by the Chairpersons of the Union and of the Commission, in which they will outline the impact of the AU and take some questions from the audience.

39. **REQUEST AUDA-NEPAD** to:

(i) Expedite the implementation of the PIDA –PAP2 projects on ICT and accelerate the implementation of the necessary policies and regulations to facilitate cross borders connectivity and regional integration;

(ii) Expand in collaboration with relevant stakeholders the cybersecurity assessments and capacity building to all AU Member States and to work with Member States to design country-specific action plans for cybersecurity and cyber-resilience;

(iii) Expand the PIDA Job Creation Toolkit to cover all ICT sub-sectors, train Member States on its usage and undertake detailed analysis of the job potential of PIDA and other significant ICT projects on the continent;

(iv) In line with the PIDA-PAP 2 Integrated Corridor Approach, incorporate ICTs, Digitalisation and Cybersecurity in the implementation of Agenda 2063 flagship projects such as the African Integrated High Speed Rail Network, the Single African Air Transport Market (SAATM) , the African Continental Free Trade Area, The Free Movement of people as well as continental initiatives such as the African Single Electricity Market (AfSEM);

40. **REQUEST THE PAPU SECRETARIAT** to put in place and implement, in coordination with the AUC, a systematic and coordinated digital transformation program to ensure that African posts are up-to-date;

41. **REQUEST** the African Telecommunication Union (ATU) Secretariat to put in place and implement, in coordination with the AUC, programmes and initiatives to facilitate a harmonized and optimum use of radio spectrum across the continent to effectively contribute to close the digital connectivity gap in Africa;

42. **APPROVE** similar initiatives for the 60th anniversary of the Organization of African Unity in 2023, whose content would trace the achievements back to 1963 instead of starting in 2002 as with the 20th anniversary;

43. **FURTHER REAFFIRM OUR REQUEST** to multilateral financial institutions and partners, including the AfDB, the World Bank and others, to continue to provide support towards making use of existing technologies to manage COVID-19 pandemic, the implementation of the Digital Transformation Strategy for Africa and the overall implementation of this Declaration.

APPRECIATION:

44. **EXPRESS** our gratitude to the AU Commission for the excellent organization of this conference.

Done on 27th October 2021

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, ETHIOPIA P. O. Box 3243 Telephone: 251 11 551 7700 Fax: 251 11 551 7844
Website: www.au.int

EX.CL/1308(XL) Annex 2

DRAFT AU INTEROPERABILITY FRAMEWORK FOR DIGITAL ID

December, 2021

CONTENTS

Executive summary

Millions of people in Africa lack legal identification (ID), and many more have IDs that are not fit for purpose in the digital age. As a result, they are facing challenges to access services and opportunities being created through digitalisation. Therefore, interoperable, trusted and inclusive digital foundational IDs, which provide people with the ability to verify their legal identity offline and online, can help to address those challenges and have significant potential to accelerate the digitalisation of African economies and societies by supporting entrepreneurship and contributing to the successful implementation of the African Continental Free Trade Area (AfCFTA). It is for these reasons that most African countries are currently modernising their ID ecosystems, although they are at different stages of doing so.

The draft AU Interoperability Framework for Digital ID (the Framework) sets out a vision that will **enable all African citizens to easily and securely access the public and private services they need, when they need them, and independently of their location.** To this end, the Framework defines common requirements, minimum standards, governance mechanisms, and alignment among legal frameworks. Its objectives include the need to:

1. allow African citizens to verify their legal identity offline and online to access public and private sector services in AU Member States;
2. empower African citizens with control over their personal data, including the ability to selectively disclose only those attributes that are required for a particular transaction. The personal information to be disclosed should be minimal, proportionate and should contain only the information relevant to that particular transaction that considered African particular situation and in line with international best practices;[2] and
3. strengthen trust and interoperability among foundational identification systems of AU Member States.

The Framework provides for a common standard at the continental level to represent, digitally, the proofs of identity issued by trusted sources from AU Member States and to ensure interoperability throughout the continent. Individuals who hold an ID from a national system will be able to obtain an interoperable, digital credential for legal identity (IDC-ID) that will take the form of a verifiable claim.[3] Standards will be established for the interoperability framework that will define key elements of the IDC-ID. These standards will operate to demonstrate trust in the IDC-ID as created under the governance of a trust framework that defines the conditions under which such credentials will be issued by trusted sources from AU Member States.

AU Member States have the freedom to select how they want to issue this digital credential. It may be stored in a purely digital format on a smartphone application, a cloud-based server, a smartcard, or a link to the digital representation may be established using a one- or two-dimensional barcode on a paper document (printed on paper, plastic card). Member States can also decide to reuse this standard to represent identity data at the national level, as part of a continental or Regional

[2] See, The *EU General Data Protection Regulation* (GDPR), 2016: https://gdpr.eu.
[3] 'Claims' are a collection of attributes about a data subject: e.g., family name or date of birth. A 'verifiable claim' is a tamper-evident version of this information which can be cryptographically verified in order to check its authenticity.

Economic Community (RECs) level, or even issued separately to complement existing digital ID systems.

The Framework will be based on the development of interoperable, inclusive, and trusted foundational ID systems as these provide the backbone of authoritative sources of data on people's legal identity and thus enable the IDC-ID to achieve higher levels of assurance. AU Member States are therefore encouraged to strengthen their foundational ID systems, taking into consideration supportive mechanisms like the *Principles on Identification for Sustainable Development*.[4] This Framework will also take into account and builds upon parallel continental efforts to create an enabling environment aiming at protecting personal data, maintaining cyber security, and safeguarding people's rights, with the adoption of the *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention)[5] and ongoing work to develop a continental data policy framework.

The issuance of the IDC-ID can be completed with an infrastructure enabling more advanced use cases such as remote authentication. This Framework highlights several technical options available to AU Member States to implement this layer. Examples include a federation of identity providers providing authentication mechanisms to the holders of the IDC-ID, the development of digital ID wallet solutions, or any other models enabling interoperability. AU Member States will also be able to seek further agreement on how to establish this authentication layer infrastructure and partner with RECs and other continental initiatives that are already investigating the introduction of interoperable foundational digital ID solutions to access services remotely.

The success of the proposed Framework is based on the assumption that it will be adopted and endorsed by AU members States. To do so, certain risks must be mitigated and addressed, and challenges must be overcome, including the risk of exclusion, weak security mechanisms, the risk of eroding personal privacy, a lack of demand (often due to uncertainties about the benefit of foundational digital ID systems), a lack of technical and financial capacities, a dearth of data centres (important for storing sensitive data) across Africa, the presence of non-interoperable ID systems, and outdated legal and regulatory frameworks. (These challenges are addressed in more depth in section 5 below.)

The document comprises of the following sections:

1. A **background** section on the work of the AU that has led to the creation of this document, an overview of the state of ID systems in Africa, and a series of initiatives promoting the interoperability of digital IDs on the continent.
2. An **introduction** to the vision, objectives, scope and potential use cases for the proposed Framework.
3. An overview of the **key elements constituting the Framework**, notably guiding principles for its design and implementation, the model selected, the key components of the framework that will have to be further defined (e.g., rules of participations, interoperability, and technical requirements), as well as three potential architectural

[4] The *Ten Principles on Identification for Sustainable Development* have been endorsed by 30 international and regional organisations, including African institutions such as UNECA, AfDB and Smart Africa, as well as adopted by a number of African countries. See: https://id4d.worldbank.org/principles.

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

options to set up an interoperability authentication layer.

4. A **high-level roadmap** elaborates on the proposed phased approach for the definition and implementation of the Framework, as well as concrete actions that might be taken by Member States and the AU.
5. High level assumptions**,** challenges, risks to be addressed, and recommended mitigation mechanisms.

The Framework does not call for the creation of a unified continental digital ID system, but calls for establishing an interoperability framework for existing foundational digital ID systems among AU Member States that takes into consideration the digital sovereignty of AU Member States, the differences in the digital infrastructure rollout, the availability of associated policies and regulations, the different types of ID systems and vulnerability of populations during and after the implementation of the interoperable digital ID systems.

Acronyms and abbreviations

AfCFTA	African Continental Free Trade Area
AML/CFT	Anti-Money Laundering/Combating Financing of Terrorism
API	Application Programming Interface
AU	African Union
AUC	African Union Commission
CIRTs	Computer Incident Response Teams
CRVS	Civil Registration and Vital Statistics
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EAC	East African Community
ECOWAS	Economic Community of West African States
GIZ	Gesellschaft für Internationale Zusammenarbeit
GSMA	GSM Association
HSMs	Hardware Security Modules
ICT	Information and Communication Technology
IDC-ID	Interoperable Digital Credential for Identity
ITU	International Telecommunications Union
KYC	Know-Your-Customer
LOA	Level of Assurance
PATF	Pan African Trust Framework
REC	Regional Economic Community
RP	Relying Party
SATA	Smart Africa Trust Alliance
The Framework	AU Interoperability Framework for Digital ID
UNECA	United Nations Economic Commission for Africa
WURI	West Africa Unique Identification for Regional Integration and Inclusion

See Annex I for working definitions.

1. Background

1.1. Context

Being able to prove one's identity is essential for their ability to access services and exercise certain rights. Traditionally, proving identity could be done on the basis of familiarity, appearance and vouching by others, which worked in smaller, informal communities. As societies and economies became larger, more formalised and more integrated, physical credentials such as ID cards and passports were introduced to establish trust. However, as countries shift to digital societies and economies, such physical credentials are not very useful for proving identity over the Internet and carrying out other digital transactions such as digital payments and sharing personal data. A prerequisite for trust online therefore are digital identities, represented by digital IDs that use modern technologies and approaches to enable people to securely prove and verify their identity online.

IDs and, in particular, digital IDs can provide a wide range of benefits for countries. Some examples include good governance, financial inclusion, gender equality and the empowerment of women, enhanced social protection, healthcare and education outcomes. For individuals, digital IDs provide a tool to assert their rights and eligibility for services and transactions. For governments and businesses, digital IDs provide a platform to streamline, expand and innovate their operations' service delivery through the use of digitalisation and automation, especially when envisioned as a 'digital stack' with trusted data sharing and digital payment platforms.[6] Considering that the Internet has no borders, digital IDs that are issued in one country and recognised in others can also be a powerful driver of social and economic integration, whether at the bilateral, regional or global levels.

Digital IDs achieve the greatest security and impact when they are based on the legal identity of individuals. Legal identity is typically managed by a country's foundational ID ecosystem, including civil registration, national ID, and other similar systems. However, millions of people in Africa are still lacking foundational identification such as a national IDs or birth certificates.[7] It is in this context that, in July 2016, the AU Assembly declared 2017 to 2026 as the decade for repositioning CRVS in Africa as a priority on the continental, regional and national development agenda. It also urged governments to respond with appropriate action.

Agenda 2063: The Africa We Want, which is the strategic framework for the socio-economic development and transformation of the continent within a period of 50 years, has called for legal identity for all. The *Digital Transformation Strategy for Africa* (DTS), endorsed at the 36th Ordinary Session of the African Union Executive Council in February 2020 in Addis Ababa, Ethiopia (EX.CL/Dec. 1074 (XXXVI), also underscored the importance of digital ID as a building block for the establishment of a

[6] COVID-19 has highlighted the importance of digital stacks as the countries with these fully or partially in place before the pandemic began were better able to quickly and effectively deliver social assistance and were more resilient when in-person services had to be moved online.
[7] World Bank (n.d.), *Global ID4D Dataset*, see: https://id4d.worldbank.org/global-dataset.

Digital Single Market (a mission that is also shared by the Smart Africa Alliance) in line with the African Continental Free Trade Area (AfCFTA).
The DTS also recognised that the development of the digital economy and society relies on important enablers, notably a strong enabling environment with regard to cyber security and data protection. The 2014 *Convention on Cyber Security and Personal Data Protection* (the Malabo Convention)[8] provides a legal, policy and regulatory framework that enables the establishment of a safe digital environment for digital transaction, e-commerce, and the transfer of personal data. Unfortunately, this legal framework has not yet been signed and ratified by the required number of AU Member States for it to enter into force, effectively limiting its efficacy.[9] Once in effect, such a legal framework will not only contribute to the promotion of the trust in the Framework and inclusion, but will also mitigate risks linked to unauthorised surveillance and discrimination, particularly for vulnerable or marginalised groups, as well as ensure accountability for implementing authorities.

1.2. **State of ID systems in Africa**

Trusted and inclusive ID systems are an enabler for many development outcomes such as eliminating poverty, promoting good governance, enabling safe and orderly migration, facilitating social protection, and promoting gender equality. They are also an important driver of digital transformation. Given the fundamental need for secure and accurate online identification and authentication, digital ID and other trust services—such as digital signatures— represent the next frontier for countries of the continent. When enabled by digital infrastructure that brings people and organisations online, digital ID and trust services can be leveraged by government and commercial platforms to facilitate a variety of digital transactions, including digital payments. At a country level, digital ID could act as a unique identifier for citizen-centric systems, making it viable to integrate systems. Together, digital ID and payments platforms provide the means to move towards cashless societies, creating productivity gains, reducing corruption and fraud, and improving user convenience and benefit.
A wide range of ID system types exist across the continent, with different levels of development linkages with service delivery. Many countries are in intermediate levels of development, with coverage gaps among vulnerable populations and nascent digital capabilities, while others have newly emerging or non-existent foundational ID systems. Overall, however, the number of countries implementing national ID systems has increased exponentially during the past two decades, driven by the desire to improve the efficiency of government payments and transfers; to enhance the integrity of elections; to improve financial sector services (via know-your-customer (KYC) and SIM registration); to enhance public security; and to promote safe and orderly migration. There is also continued momentum to reform and modernise system design and implementation approaches in line with the

[8] AU (2014), *Convention on Cyber Security and Personal Data Protection*, see: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[9] As of July 2021, 14 Member States out of 55 have signed the *Malabo Convention* (*ibid*), among which 10 Member States have ratified it. To enter into force, ratification by at least 15 Member States is required.

expanding evidence on good practices and lessons learnt from successful ID programmes elsewhere.[10]

A good example is arguably provided by Rwanda, that has conducted a campaign to digitise its economy and empower its middle class by conducting actions like the move to a cashless economy, which the government aims to achieve through ubiquitous mobile phone penetration and high-speed Internet access. Rwanda joined the Better Than Cash Alliance, a global partnership committed to moving from cash to digital payments. Rwanda is already realising increased efficiency and revenue by eliminating collection costs and other expenses. It has also become a knowledge-leader in the region, and is sharing best practices with others who are interested in pursuing a similar path.[11]

The digital capabilities of ID systems have increased greatly, although digital identification in the context of online transactions is still in its infancy. Over the past decade, many countries have embarked on efforts to modernise their identification systems, with the goal of creating a digital platform and issuing credentials that underpin a variety of uses and services. These reforms frequently involve a transition from paper-based toward digital systems using electronic data capture and data management. They also commonly involve introducing digital ID verification and authentication mechanisms – for now, mostly in the context of in-person transactions. The majority (85%) of African countries have national ID systems underpinned by an electronic database, although many still rely on paper-based civil register and processes, and many systems offer limited utility for service delivery. Biometric data is collected by more than 70 percent of African countries at the time of registration to ensure the uniqueness of identities. Although some countries – such as Kenya, Lesotho, Nigeria, Rwanda, South Africa – offer digital ID verification services (to government ministries, banks, etc.) to validate identity information or credentials against a central database, authentication for most transactions continues to rely on the manual inspection of physical ID cards. Digital ID solutions that enable secure authentication for online services and transactions are still in their infancy on the continent, with such services only available in a handful of countries (e.g., in South Africa by banks, or in Cabo Verde and Seychelles for eGovernment services). Despite many improvements and the launch of new systems in recent years, African countries and their residents face several challenges when it comes to identification. Some of the key areas that required strengthening include the accessibility of ID systems, their ability to effectively support service delivery, and the implementation of safeguards that promote trust and data privacy.

Ensuring universal accessibility of ID systems is an ongoing challenge. An estimated 1 billion people around the world lack basic identity documents – and approximately half of that population reside in Africa.[12] Africa is also home to 8 of the 10 countries with the largest ID gender gaps globally and ID coverage among adults in Sub-Saharan Africa is close to 10 percentage points lower among women than

[10] A 2018 survey of African government officials revealed that 60 percent of African countries were planning to launch an ID system or modernise the existing one by the end of 2020.
[11] ITU/DIAL (2019) *SDG Digital Investment Framework*, see: https://www.itu.int/pub/D-STR-DIGITAL.02-2019
[12] ID4D (2018) *ID4D Global Dataset*, see: https://id4d.worldbank.org/global-dataset

men.[13] Challenges in identification start from birth: 100 million children under the age of five in Africa have not had their birth registered.[14] The reasons for these coverage gaps are manifold and include high direct and indirect costs of enrolment, including the cost of travel to often-distant registration sites; complex documentary and administrative requirements for registration; and limited demand where ID systems offer limited value in terms of facilitating access to services.[15]

The use of modern technologies has also increased complexity and presented new risks. For example, not all digital ID solutions are well-adapted to local needs and contexts where Internet connectivity, access to electricity, or digital literacy among civil servants or the general population may be limited. Vendor lock-in is also a common concern, and is often associated with unsustainably high operating costs, limited interoperability of the ID system, and low levels of government and individual oversight and control over identity data. In addition, with the increased adoption of digital technologies in identification and authentication as well as the shift toward digital credentials, people with limited (digital) literacy skills and access to connected devices risk being left further behind.

As systems and data processing become digitised, the need to implement effective safeguards to protect data and individuals' privacy has increased. Inadequate safeguards for data protection, privacy, and user rights – whether legal, institutional, or technological – can leave ID systems vulnerable to breaches and people's data unprotected. Many countries still have a long way to go in building secure and trusted ID systems: only 28 countries (50%) in Africa have reportedly adopted data protection and privacy legislation and 39 (70%) African countries have cybercrime legislation in place.[16] Even where and when such frameworks do exist, translating legal provisions into effective institutional, operational, and technical controls can be challenging. As of today, only a few countries store and manage their data according to international best practices to protect against theft or unintentional data loss, for example.[17]

Digital ID systems are faced with similar challenges as digital ecosystems development. These challenges include funding issues, because funding cycles (mainly donor-based ones that are project-based and time-bound), tend to be disconnected from tech development cycles. There is also often a lack of funding available for scaling up ICT, as funds tend to be available only for the stages of the technology development life cycle, with limited funding available for scaling up at national level. Besides funding and financing, planning tends to happen in silos and decision-making across stakeholder groups lead to limited opportunities for coordination among stakeholder groups. Such siloed approaches tend to limit the

[13] ID4D (2017) *Findex Survey 2017*, see: https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf
[14] UNICEF (2019) *Birth registration for every child by 2030*, see: https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf.
[15] World Bank (2017) *The state of Identification Systems in Africa*, see: https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf.
[16] UNCTAD (n.d.) *Data Protection and Privacy Legislation Worldwide* (database), see: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.
[17] World Bank (2017) *The state of Identification Systems in Africa*, see: https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf.

reuse of digital solutions and undermine their potential applicability across programmes and sectors. Deficiencies in digital literacy, including lack of capacity in ICT leadership, and in the selection, design, implementation, scaling up, and maintenance of ICT solutions, are often an issue among governments and development practitioners. [18]

1.3. **Other initiatives promoting mutual recognition and interoperability of digital IDs in Africa**

A number of existing initiatives complementary to the Framework promote the mutual recognition and interoperability of digital IDs in Africa. These include, but are not limited to:

1.3.1. Digital Transformation Strategy for Africa (2020-2030)

Digital ID is recognised as one of five cross-cutting themes of the Strategy, which also makes ten policy recommendations and proposes actions across two themes of ensuring inclusion, security, privacy and data ownership, and supporting interoperability and neutrality. While these recommendations mainly cover the development of *national* digital ID systems, one recommendation does call for the establishment of a "continental interoperable and open digital ID, allowing validation and authentication of individuals," while another recommendation requests the AUC, United Nations Economic Commission for Africa (UNECA), and other partners to "work together on continental and regional standards, including on authentication protocols, minimum data fields, deduplication protocols, biometric formats as well as other formats, model regulations, and other standards".

1.3.2. UNECA initiative on Digital ID

UNECA has launched an initiative on digital ID, trade and digital economy (DITE), acting as a Centre of Excellence, which aims at harmonising related standards, adopting regulations to safeguard security, upping investments, and developing the capacity and skills of key actors.[19] The ECA Digital Centre of Excellence supports the work aiming at establishing a harmonised Framework, defining and shaping policies and standards for digital ID, providing capacity development for Member States, RECs, and the AU. The ECA has also produced a white paper on a framework for digital interoperability through the establishment of a Pan African Trust Framework (PATF).

1.3.3. Smart Africa Trust Alliance (SATA)

Smart Africa is an initiative of African Heads of State to accelerate the socio-economic development in Africa by leveraging ICT. In 2020, Benin championed a Smart Africa flagship project to develop the Digital ID Blueprint, supported by a working group that included Rwanda, Tunisia, the AU, the International

[18] ITU/DIAL (2019) *SDG Digital Investment Framework*, see: https://www.itu.int/pub/D-STR-DIGITAL.02-2019.
[19] UNECA (n.d.), *DITE for Africa*, see: https://www.uneca.org/dite-africahttps://www.uneca.org/dite-africa.

Telecommunications Union (ITU), the World Bank, Omidyar Network, UNECA, the GSM Association (GSMA), the World Economic Forum, the Gesellschaft für Internationale Zusammenarbeit (GIZ), and several private companies. It was adopted by the Smart Africa Board, including its 32 Member States, the AU, and the ITU. The Blueprint[20] proposes SATA as a platform to facilitate the trusted recognition of digital IDs between a range of actors through federated certification mechanisms. Pilot projects of SATA are anticipated to take place in Benin, Rwanda, Tunisia, and other Smart Africa Member States. SATA will serve as an agile and adaptable solution to enable interoperability between various public and private identity schemes on the continent. More details will be available on sata.smartafrica.org.

1.3.4. West Africa Unique Identification for Regional Integration and Inclusion (WURI) program

WURI[21] is a regional program leveraging financing from the World Bank to increase access to services in participating Member States from the Economic Community of West African States (ECOWAS) by building foundational ID systems that are accessible to all persons in the territory of the country—without consideration for nationality or legal status—and are designed with cross-border interoperability in mind to unlock access to social, health, financial and other services across borders. Côte d'Ivoire, Guinea and the ECOWAS Commission joined in phase one during 2018, and Benin, Burkina Faso, Niger and Togo joined in phase two during 2020. Key principles of WURI include universally accessible and inclusive registration, data minimisation, and basic credentials that are provided at no cost to the population.

1.3.5. EAC Common Market Protocol

Through Article 8 of the Protocol, the six East African Community (EAC) Partner States have committed to work progressively towards "…a common standard system of issuing national identification documents to their nationals."[22] This is strongly linked to achieving other objectives of the Protocol, including the free movement of goods (Article 6), persons (Article 7), labour/workers (Article 10), services (Article 16), and capital (Article 24), as well as the rights of establishment and residence (Articles 13 and 14, respectively). However, the national ID systems are at varying stages of development. Nonetheless, in the spirit of variable geometry and as an initiative of the National Corridor Integration Projects (NCIP), Kenya, Rwanda and Uganda began recognising each other's national ID cards as valid travel documents in 2014. Within the framework of NCIP there have been discussions to build on this for additional use cases such as e-services, but these have not yet materialised. In 2018, the World Bank and EAC secretariat conducted a study on options for mutual recognition of national IDs (NIDs) in the EAC, and proposed four milestones.

[20] Smart Africa (2020, October) *Blueprint | Smart Africa Alliance – Digital Identity*, see: https://smartafrica.org/knowledge/digital-id/.
[21] World Bank (n.d.) *West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program*, see: https://projects.worldbank.org/en/projects-operations/project-detail/P161329.
[22] EAC (2020), see: https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png.

1.4. **Digital and Data Sovereignty**

With 55 sovereign nations, Africa has 55 legal jurisdictions to be considered when developing policy instruments. Digital sovereignty describes a spectrum of different technical and regulatory concepts, ranging from the physical location of servers and the construction of undersea cables, to laws and practices pertaining to cybersecurity, data protection and the taxation of data markets, that enable States to make their own decisions on technological choices and their regulation.
In order to guarantee digital and data sovereignty,[23] AU Member States are encouraged to:

1. establish secure storage systems for personal data (including sensitive data) by designing and setting up national data centres which must provide for data control by the State and include at least storage and processing space devoted exclusively for personal and sensitive data. It will be necessary to put in place required safeguards (technical, in particular) to ensure that data which are used in cross-border information exchanges do not in any way include personal or sensitive data whose processing or storage would pose risks to the rights of individuals or the sovereignty of AU member States.

2. build capacity and infrastructure for the development of African talents and skill sets to meet the new challenges and strengthen the digital sovereignty. Member States are expected to take the lead in advancing the skills (including cyber resilience skills) of all citizens and residents, and should empower people to have control over their personal data.

3. establish partnership based on mutual respect, win-win situation without compromising sovereignty and national ownership and avoids foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States

The Framework will be guided by the sovereign rules represented by each AU Member State's registration and identity issuing authority or authorities, and the proposed governance structure including the establishment of a continental coordinating institution to be endorsed by AU Member States. Furthermore, accountability mechanisms including the handling of liabilities in case of misconduct will be defined and endorsed by AU Member States. Developing continental trust among sovereign states with divergent digital identification schemes is a complex but achievable task requiring multi-stakeholder collaboration. To achieve interoperability for the exchange of legal identity information in respective African countries, the commonalities between existing national rules and standards must be recognized, based on a minimum set of criteria which will allow both local sovereignty and sufficient trust in each other's approach.
For this purpose, AU Member States need to strengthen and enhance their legal frameworks and enforcement capacities, in particular the capacities of data protection authorities in monitoring cross-border data transfers and enforcement of relevant laws and regulations in cases of breaches or misuse.

The proposed Framework will embrace state-of-the-art technologies and be respectful of countries' laws and regulations. Governments are not obliged to use

[23] 'Data sovereignty' as used in this Framework has the following meaning: personal data (including sensitive data) related to digital identification systems in an AU Member State must be collected, stored and processed (i) in facilities owned or controlled by and (ii) under the applicable law of the AU Member State.

specific technologies. The use of open standards and norms will guarantee a large diversity of technological choices by the States while facilitating country ownership and interoperability.

2. Introduction

In 2020, AU Member States adopted the Digital Transformation Strategy (DTS) for Africa (2020-2030) with the vision of establishing:

> *An Integrated and inclusive digital society and economy in Africa that improves the quality of life of Africa's citizens, strengthen the existing economic sector, enable its diversification and development, and ensure continental ownership with Africa as a producer and not only a consumer in the global economy.*

Realizing this ambition – as well as that of the AfCFTA – depends on the development of inclusive and trusted foundational digital ID systems that enable all African citizens to prove and verify their legal identity reliably and securely when transacting in-person and online, and enable public and private sector service providers to recognise identity credentials, no matter where in Africa they have been issued. Importantly, foundational digital ID systems must be designed to empower people, especially disadvantaged and marginalised populations. This will enable all African citizens to meaningfully participate in the digital economy and society, to unlock access to services within countries and across borders, to promote trade as part of the AfCFTA, to enhance trust in the digital society and economy, and to reduce fraud and costs of doing business in and with Africa.

Importantly, foundational digital ID systems can also underpin the development of broader 'digital stacks'[24] with digital payment and trusted data sharing platforms to create opportunities for innovation and a wide range of presence-less, paperless and cashless transactions across the continent. However, this also requires risks related to exclusion, data protection, cybersecurity and technology, and vendor lock-in to be comprehensively mitigated. It is for these reasons that digital ID is one of five cross-cutting themes of the DTS, providing the mandate and setting for this Framework.

2.1. Vision, objectives and indicative use cases

The vision of the AU *Interoperability Framework for Digital ID* is that all African citizens in Africa can easily and securely access the services they need, when they need them, from both public and private sector providers, which will encourage inclusive and meaningful participation in the wider digital economy and society and allow services to operate with greater trust and certainty.

To this end, the Framework defines common requirements, minimum standards, norms, governance mechanisms, alignment among legal frameworks with the objectives to:

1. allow all African citizens to **verify their legal identity offline and online** to access

[24] In the context of digital technologies, a 'stack' is a collection of independent software components or infrastructure that work together to support the execution of a use case.

public and private sector services in all participating AU Member States;
2. empower all African citizens with **control over their personal data**, including the ability to selectively disclose only those attributes that are required for a particular transaction. The personal information to be disclosed should be minimal, proportionate and should contain only the information relevant to that particular transaction; and
3. strengthen **trust and interoperability** among foundational identification systems of AU Member States.

The Framework does not call for the creation of a unified continental digital ID system, but provides a foundation for interoperability between existing digital ID systems of AU Member States that takes into consideration the digital sovereignty of AU Member States, the differences in the digital infrastructure rollout, the availability of associated policies and regulations, the different levels ID systems and vulnerability of populations during and after the implementation of digital ID systems. It is paramount that this Framework is developed in line with best practices and international norms[25] aimed at protecting personal data, maintaining cybersecurity, and safeguarding people's rights. With the adoption on the Malabo Convention,[26] the AU has taken an important step towards establishing a credible digital environment for online transactions via the adoption of a common set of rules to govern the cross-border transfer of personal data across the continent and the alignment of national data protection and cybersecurity frameworks.

A continental Framework can facilitate **access to services in all participating countries by enabling people and businesses** to verify credentials and other facts without disclosing personal data. This includes the possibility to authenticate identity when accessing online services (e.g., government services) in another country with their digital ID without the need to enrol in the local foundational identity solutions recognised by foreign service providers. The interoperability of digital ID also facilitates the sharing of and consent for verifiable credentials and trusted data when applying for services where the law demands such verification (e.g., proof of insurance, qualification vaccination status); enabling people to save time and reduce red tape.

It can also **enhance the integrity and accessibility of cross-border payments and financial services in Africa, and create opportunities for innovation**. Weak and untrusted ID systems, coupled with the absence of harmonisation of rules, create anti-money laundering/combating financing of terrorism (AML/CFT) risks,[27] which introduce barriers to cross-border exchanges, raise costs of services (e.g., remittances), and hamper innovation. Digital ID can facilitate customer identification and verification at on-boarding, support KYC processes, and aid the monitoring of transactions for the purpose of detecting and reporting suspicious transactions.

---

[25] This includes among other policy instruments, the *Convention on Cybercrime of the Council of Europe* (CETS No.185), known as the *Budapest Convention on Cybercrime*, see: https://www.coe.int/en/web/cybercrime/the-budapest-convention; ISO/IEC 29151, see: https://www.iso.org/standard/62726.html; the *UN Principles and Recommendations for Vital Statistics Systems*, see: https://unstats.un.org/unsd/demographic/standmeth/principles/m19rev3en.pdf; international norms on data protection (such as the GDPR and Council of Europe Convention 108+); global and regional standards and trust frameworks for identification.

[26] AU (2014) *Convention on Cyber Security and Personal Data Protection*, see: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[27] AML/CFT risks refer to anti-money laundering and counterterrorist financing risks. The Financial Action Task Force (FATF) recommends to governments that they develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID and developing regulations and guidance to mitigate those risks.

Interoperability will not only make it easier for migrants to send money home by easing the KYC verification and the authentication burden, it will also help to lower costs, helping Africa to move closer to the SDG target (10.c) of three percent by 2030.

A continental Framework can also **strengthen trade and e-Commerce by increasing trust in online commercial transactions and make it easier to do business and trade across Africa**. In 2020, intra-African trade represented only approximately 16.6% of Africa's GDP.[28] The AfCFTA was launched in 2019 to unlock new opportunities for trade and eCommerce by 2030. Cross-border recognition of digital IDs can aid stronger identity checks of buyers and sellers, especially for restricted goods sold online. It can also enable e-signatures for online, paper-less transactions, which enable businesses and clients to save time and increase security by reducing risks of identity fraud. It also simplifies doing business across borders, by enabling businesses to manage their interaction with government digitally, for example declaring tax, participating in procurement procedures, requesting VAT numbers, and applying authorizations.

2.2. **Scope**

To achieve these objectives, the Framework will define:

- the **type of information/data** that can be shared in the form of a minimum dataset for foundational identity information;[29]
- the **way of proving who issued the data** and that it can be trusted by;
    - establishing a process to communicate trusted authoritative sources[30] for identity data in each AU Member States; *and*
    - determining how to verify the authenticity of the digital claim; *as well as*
- the standards and processes that describe **how data is shared** by users and verified by others in offline and online environments.

This document outlines the foundations of a trust and interoperability framework for digital ID systems across the African continent. It will define the minimum requirements necessary to ensure interoperability between existing and future digital ID systems. Interoperability refers to the ability of different parties of the Framework – such as digital ID systems and the systems of relying parties – to communicate and interface effectively at technical and semantic levels. Interoperability can facilitate mutual recognition, which is a legal construct, but is not a prerequisite, and nor does it guarantee mutual recognition. The Framework does not define a unified digital ID system for Africa and does not address commercial and liability agreements between participating Member States.

Many African countries already have digital ID systems well underway and some have introduced digital authentication capabilities. **The Framework provides common requirements for communicating foundational identity data and processes that would be interoperable and accepted in other African Member**

[28] UNCTAD (2019) *Economic Development in Africa Report 2019*: Made in Africa: Rules of origin for enhanced intra-African trade, see: https://unctad.org/press-material/facts-figures-0.

[29] Although the scope of this document focusses on identity data, the proposed trust framework can be extended by AU Member States to represent other proofs and achievements, such as diplomas, professional qualifications, etc…

[30] Member States will maintain legal responsibility and accountability relative to the trusted authoritative sources (data issuers).

States, while Member States retain full control and choice for the design of their national systems.

The Framework complements and builds on, rather than duplicate activities associated with the Protocol to the *Treaty Establishing the African Economic Community Relating to Free Movement of Persons, Right of Residence and Right of Establishment, and the Conference of African Ministers Responsible for Civil Registration and the African Program for Accelerated Improvement of CRVS* (APAI-CRVS). Implementation of the Framework should be closely coordinated with this and other relevant initiatives, such as to explore migration as an additional use case for digital IDs at the appropriate time and to ensure that the coverage and quality of CRVS systems are improved as an important input for digital foundational ID systems.

2.3. **Trust framework, Data Privacy, Interoperability and Standards**

Identity systems should foster trust between the various participating parties, ensuring that the legal rights of both individual users and operating agencies are observed, and that the ethical use of identity systems is promoted. **To ensure this trust, a set of rules that all parties sign up to and observe** must be defined; a Trust Framework.

Whilst technology acts as a key enabler, Trust Frameworks also focus on process and procedure. A robust trust framework should clearly define the:

- **Business requirements** (e.g., scope, services provided, requirements for participation);
- **Technical requirements** (e.g., data formats, interfaces, standards);
- **Operational requirements** (e.g., how identity proofing and authentication work, support, communications); *and*
- **Legal requirements** (e.g., service levels, liability, dispute resolution, recognition of e-transactions legally within countries) for the identity system.

The Framework is based on **interoperability**. To facilitate interoperability, one entity must be able to trust another entity based not only on the integrity of technical processes (e.g., cryptographic proof, etc.), but also regarding the provenance of the data being shared (e.g., the processes for its collection and for attributing a certain record to an individual).

Interoperability does not require that foundational ID systems be uniform, but simply that certain common and open standards are followed. Under the Framework, each participating country can create foundational ID systems adapted to their local needs, traditions, and legislation, as long as certain standards that enable interoperability are followed. Open **standards** establish universally understood and consistent interchange protocols, testing regimes, quality measures, and good practices regarding the capture, storage, transmission, and use of legal identity data, as well as the format and features of legal identity credentials and authentication protocols. When considering interoperability of digital ID credentials and authentication across the continent, it will be important to consider open standards for the identity claims, how they are issued, and how trust is communicated between the entities involved in

the Trust Framework. These claims, which will form the **basis for legal digital ID,** will often originate from authoritative sources such as government agencies. An authentication mechanism must also be defined to enable legal digital ID holders to share these claims with services providers appropriately, ensuring that disclosure of data is binary and any metadata is anonymous, as well as the privacy and rights of individuals protected at all times.

This framework will define **how the trust can be established in these verifiable claims, and how governance elements and standards for data operate**. The technical implementation of the solution can be driven by the market, which will be able to leverage the trust framework to develop innovative digital foundational ID solutions. The Framework places data privacy, auditing and data protection at the centre and lays a transparent procedure to be applicable to all involved relying parties on how data is requested, gathered, transmitted and stored. It follows well-accepted standards on information/data sharing procedure. The importance of tokenisation in reducing the opportunities for data harvesting, cloning and fraud, by presenting the ID holder with the functionality to issue virtual IDs in order to protect the actual IDs itself, is additional aspect that will be further elaborated to strengthen the data privacy at national/continental level.

3. The Framework

The *AU Interoperability Framework for Digital ID* proposes to define, at the continental level, a harmonised approach for individuals to share digital ID claims[31] issued by trusted authorities with service providers in order to prove their legal identity in an online and offline environment. It will consist of agreeing on a **common standard to represent existing proofs of legal identity issued by AU Member States in a digital format**.[32] The authenticity of such credentials[33] would be able to be verified in order to guarantee a high level of trust and security.

There are no restrictions placed on national foundational identity systems, how they operate or which types of credentials they use to authenticate individuals; each country is sovereign in this respect. The intention of the framework is to create conditions for interoperability at a continental scale, building on and extending the reach of existing systems where they exist, rather than restricting their use.

The interoperable digital ID credentials (IDC-ID) issued in line with the Framework will take the form of a verifiable claim that will be complementary to existing national foundational ID systems and regional cooperation projects, without replacing the domestic digital identification systems of AU Member States. **AU Member States remain free to select how they want to issue this digital credential**. It may be

[31] 'Claims' are a collection of attributes about a data subject: e.g., family name or date of birth. A 'verifiable claim' is a tamper-evident version of this information which can be cryptographically verified in order to check its authenticity.
[32] The current framework focusses on the definition of verifiable claims to prove identity data but could be expended to share verifiable claims about academic achievements, professional qualifications, etc.
[33] A 'credential' is composed of an identity claim, metadata about the issuer, and a proof of authenticity, which is usually a digital signature.

stored in a purely digital format on a smartphone application, a cloud-based server, a smartcard, or a link to the digital representation may be established using a one- or two-dimensional barcode on a paper document (printed on paper, plastic card).
The Framework is based on the development of interoperable, inclusive and trusted ID systems as these provide the backbone of authoritative sources of data on people's legal identity and thus enable the IDC-ID to achieve higher levels of assurance. AU Member States are therefore encouraged to strengthen their ID systems, potentially drawing upon the *Principles on Identification for Sustainable Development*.[34] Alternative solutions to obtain an IDC-ID for people that are currently excluded from an ID system can be considered.
The standards for an interoperable legal digital ID could be used at the domestic level or support cross-border use cases. For example, the standard could be adopted to:

- represent foundational digital ID data at the national level on newly issued or updated digital ID credentials; or
- represent foundational digital ID data at continental or REC level; or
- be issued separately in complement to pre-existing foundational digital ID systems.

The interoperability, trust, and inclusivity elements defined as part of this framework constitute a launch pad for a more comprehensive continental framework and infrastructure for digital identification and authentication on the continent.

3.1. **Guiding Principles**

The following principles shall guide the cross-border interoperability implementation of the Framework:

1. Transparency in governance and operation.
2. Easily accessible, cost-effective, operationally sustainable, and widely usable.
3. Promote, respect, and uphold human rights and freedoms.[35]
4. Ensure technical integrity, including unique, secure, scalable, and accurate identity.
5. Guarantee the sovereignty of Member States, ensuring data sovereignty. Notably, digital ID data belongs to, and remains in the control of Africa.
6. Be interoperable among AU Member States.
7. Use open standards[36] and prevent vendor and technology lock-in.
8. Protect data privacy and enable people to control their personal data, including data proportionality through system design.
9. Safeguard data privacy, security, and rights through a comprehensive legal and regulatory framework.
10. Establish clear institutional mandates and accountability.

Considering that the Framework depends on authoritative sources, such as legal identification systems, the quality and coverage of these systems therefore has an

[34] The *Ten Principles on Identification for Sustainable Development* have been endorsed by 30 international and regional organisations, including African institutions such as UNECA, AfDB and Smart Africa, as well as adopted by a number of African countries. See: https://id4d.worldbank.org/principles.
[35] As per the *African (Banjul) Charter on Human and Peoples' Rights* (Adopted 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21 October 1986).
[36] 'Open standards' are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (*adopted from ITU-T*).

impact on its implementation. Exclusion from these systems and other challenges such as weak security, for example, will lead to the same in terms of the ability to issue and properly use credentials.

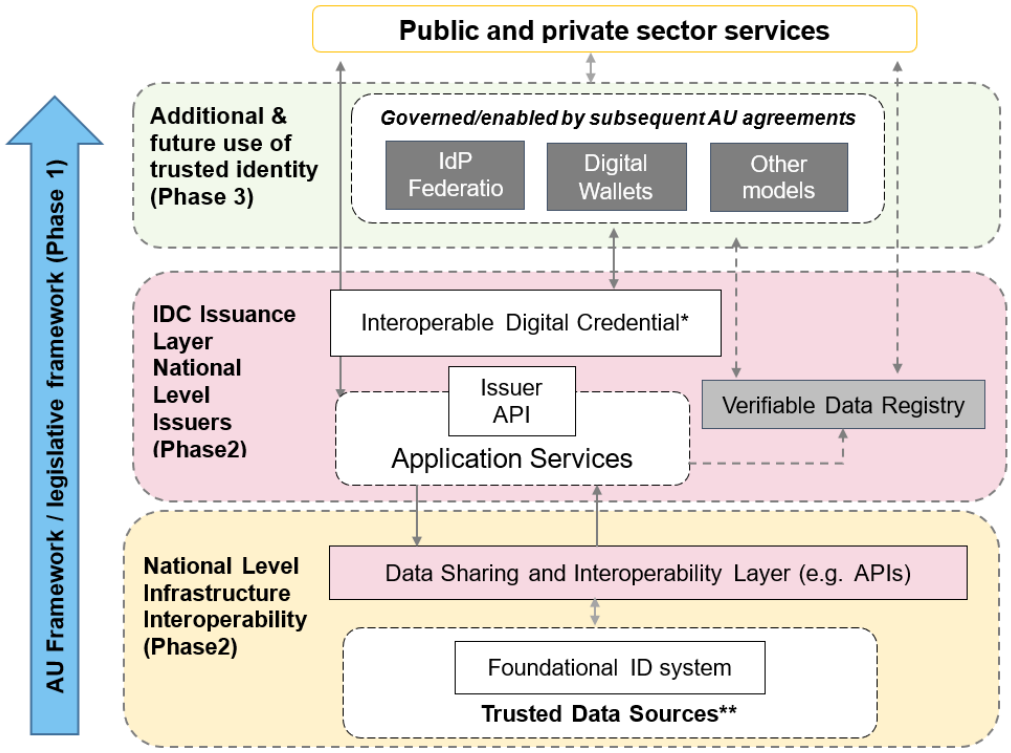
Therefore, AU Member States should meet their obligations to ensure that all people present in their territory have access to legal identification, in line with the Convention on the Rights of the Child and other international and regional legal instruments. Furthermore, they are also strongly encouraged to adhere to existing relevant international norms[37] and principles[38] and ensuring that authoritative sources, and especially their legal identification systems, are inclusive, protective of people's data and rights, and designed to support the continental economic and societal integration.

3.2. **The model**

The Framework proposes implementation in three phases:

1. Adoption of the Framework and development of an enabling legislative framework;
2. Implementation of the framework and adoption of technical specifications for the IDC-ID;
3. The scale-up of the implementation of the framework and the provision of an infrastructure that enables more advanced use cases such as remote authentication.

Figure 1 – Phased implementation approach to the Framework



[37] This includes among other policy instruments, the *Convention on Cybercrime of the Council of Europe* (CETS No.185), known as the *Budapest Convention on Cybercrime*, see: https://www.coe.int/en/web/cybercrime/the-budapest-convention; ISO/IEC 29151, see: https://www.iso.org/standard/62726.html; the *UN Principles and Recommendations for Vital Statistics Systems*, see: https://unstats.un.org/unsd/demographic/standmeth/principles/m19rev3en.pdf; international norms on data protection (such as the GDPR and Council of Europe Convention 108+); global and regional standards and trust frameworks for identification.

[38] Such as the *Ten Principles on Identification for Sustainable Development*, which have been endorsed by 30 international and regional organisations, including African institutions such as UNECA, AfDB and Smart Africa, as well as adopted by a number of African countries. See: https://id4d.worldbank.org/principles, and the *Principles on Digital Development*, which have been endorsed by 200+ organisations, see: https://digitalprinciples.org/.

* *Implementation details of phase 2 will be further discussed with AU Member States.*

** *Member States will decide what trusted data sources entail their foundational ID systems.*

The IDC-ID shall ensure that **issuing authority does not know which services individuals access with their digital ID**, but authenticity of the identity credentials can be checked. This provides safeguards in terms of data protection and privacy and more control to the individual on how his or her data is used.
The infrastructure layer will enable more advanced use cases and will operate by binding identity credentials issued in the IDC-ID format to the actual individuals. Several technical options are available to AU Member States to implement this layer, including a federation of identity providers providing authentication mechanisms to the holders of the IDC-ID, or the development of digital ID wallets solutions, or any other models enabling interoperability. Each of these implementations can offer **data minimisation and selective disclosure services** for specific use cases, for example by only sharing the relevant data points from an ID card and credit report to obtain a loan, seek social or health benefit, obtain a pension benefit, apply for scholarships, or anonymise the IDC-ID minimum dataset (name, date of birth) into a proof of majority (+18y or +21y or a yes/no response).

3.2.1. Architecture Components

Trusted data sources must meet standards set by the Framework for data quality and integrity. In many cases, this would be fulfilled by a foundational ID system (whose trusted data sources will be decided by Member States) that can provide a proof of legal identity.

Figure 1 depicts the extending of access to existing national systems and trusted data sources through a data sharing and Interoperability layer based on standards and protocols enabling trusted IDC Issuance. Services providers will be required to verify and retrieve legal identity data when creating foundational digital ID credentials.

The IDC Issuance Layer depicts the standardised issuance of IDC credential based on a foundational/national level ID system trusted data source. Each credential Issuer (at least one per participating member state) will have a number of key functions (not limited to the following):

- An Issuer API that enables wallets and other systems to request and retrieve credentials;
- A Verifiable Data Registry that enables the verification of identifiers and credential revocation checking;
- Cryptographic Key Management;
- Visibility and Auditability of credential use for the Holder of an IDC credential;
- Providing Credential Metadata alongside each issued credential to describe the quality, provenance, and level of trust associated with the issued credential.

3.2.2. National level and interoperability requirements

There is no requirement for existing identity systems at the domestic level to be reengineered to achieve interoperability at the continental level. Instead, standards for the interoperability of data, technical interoperation via application programming interfaces (APIs) and protocols, and the technical representation of credentials will be adopted. The issuance of credentials, as well as their creation, is logically separate to existing national systems but would be under the control of nationally responsibly agencies.

Technical trust, underpinned by advanced cryptography, may not require a continental PKI or other super-national infrastructure, but would instead stem from AU Member State preference and/or capability; utilising either national PKI (where used) or legally recognised alternatives. Each AU Member State will continue to exercise national sovereignty in the design of national identity systems, including how those systems interoperate with the AU Framework.

3.2.3. Standards for the participation of trusted data sources

Standards will be set under the Framework for the quality, security, reliability, and minimum level of assurance associated with each trusted data source. Member state systems should provide evidence that they have reached the minimum requirements for participation before they are able to participate in the Framework and issue IDC-compliant credentials. The nature of these standards will be determined by agreement of the AU member states.

3.3. **Trusted process – the Trust Framework**

The Trust Framework should describe clear rules for the participation of entities (e.g., issuers, holders, and verifiers of identity), the operation of the Framework, and the technical requirements for interoperability of trusted credentials.
This will enable all entities to trust the credentials shared by holders of identity based on the trust established by the issuing authority (for the credential) and the processes each entity has agreed to adhere to under the Trust Framework.
It is expected that the following key sections would be drafted by the Member States as part of the Trust Framework.

3.3.1. Roles and Responsibilities

A clear definition of each entity (e.g., an issuer of credentials), and the responsibilities it has for trust to be maintained, such as the safe and secure management of data and services, and incident reporting.
Key roles expected to be included in the Trust Framework would be that:

- The **trusted authorities** are authoritative sources of data for legal proof of identity as endorsed by AU Member States.
- The **issuers** are entities responsible for issuing the proof of legal identity in the

standardised digital format under the Framework to the holder. Trusted authorities can either issue the credentials themselves or mandate another entity with a more adequate skillset (e.g., ICT agency, private sector).

- The **holder** of the IDC-ID is the individual that possess one or more digital credentials. The holder can (but not always) be the **subject** of the identity attributes shared via the IDC.
- The **verifier** is a relying party (e.g., public or private service provider) that wants to verify the identity claim of a given subject.
- **Identity providers, credential providers, and digital wallet providers** can further contribute to the ecosystem by providing an authenticator to bind the identity of the holder to the credentials and therefore enable more advanced use cases requiring remote authentication.

An independent Supervisory Body to be established by Member States may be necessary to ensure that participating entities remain compliant with the rules laid down by the trust framework and set minimal tools and technologies required for compliance. The Supervisory Body should also be entrusted with the task to raise awareness in cyber resilience skills across the continent to ensure sustainability of the framework.

3.3.2. Rules for Participation

Rules for participation may include minimum legal, operational, or organisational requirements required for a trusted authoritative entity providing a service under the Trust Framework. For example, an Issuer may be required to have official authorisation to operate (from an authoritative source / government agency). Services accepting IDC-ID may be requested to confirm their conformance with baseline data protection, privacy, and redress (for identity holders) requirements. An MoU may also be required to ensure that all operating entities agree with the terms of the trust framework.

3.3.3. Governance

Governance mechanisms to be endorsed by AU Member States will be required to set and maintain the rules of the Trust Framework, approve changes to the interoperability requirements, and to delegate responsibility for the drafting/development of changes to the Framework to governance sub-groups as necessary.

An Independent Supervisory Body to be established by AU Member States may be necessary to ensure that participating entities remain compliant with the rules laid down by the Trust Framework. This entity should also be responsible for ensuring that all parties satisfy formal compliance to standards and, should they deviate, are audited or brought to account as deemed necessary, for example, in the case of a data breach.

The protection of individuals should be paramount. The Supervisory Body should be empowered to receive and act upon complaints by IDC-ID holders affected by poor practice, data breaches, identity fraud, or other incidents related to digital ID. It

should also be the focal point for mechanisms of redress even if this is only a coordinating role and should act as a champion of individuals and their rights.

3.3.4. Interoperability Requirements

3.3.4.1. **Levels of Assurance**

A means of communicating the level of trust in a credential presented by a Holder to a Verifier. The Framework should define the conditions by which each level can be achieved based on the verification of identity by an authoritative source, the process of issuance, and the means of holding and presenting a credential.

3.3.4.2. **Minimum Dataset**

The minimum amount of data regarding the identity of a holder as provided in an identity credential, should be adequate for the identification of the individual in the majority of common transactions whilst respecting the need for data minimisation. Attributes contained in the minimum dataset can be provided by different trusted entity.
The governing body is at liberty to define how additional claims (datasets) may be included optionally in the trust framework. Any issuance of corresponding credentials should be subject to the same conditions and rules as issuers of foundational identity credentials.

3.3.5. **Technical Requirements**

3.3.5.1. **Security**

Baseline security requirements should be defined for each entity providing a service as part of the identity infrastructure.

3.3.5.2. **Cryptographic proof**

Credentials will be verified by the inclusion of a digital signature created by the issuing authority. Checking the validity of the signature acts as a cryptographic proof that the claim made by the Holder presenting the credential can be trusted. In order to check, a digital signature public key will be required. The public key may be provided through a decentralised or centralised method to be determined as part of the Trust Framework and its technical requirements.

3.3.5.3. **Credential format**

Technical specifications for the creation and transmission of credentials should be defined, drawing on existing standards such as W3C Verifiable Credentials where applicable.

- The **Interoperable Digital Credential for Identity (IDC-ID)** is a set of legal identity

claims (e.g., attributes) and relationship made by an issuer that can be cryptographically verified. More specifically it includes:

- Credential metadata about the type of credential issued, date of issuance, and name of issuer;
- Information about the subject of the claim and the actual legal identity claim (e.g., date of birth).
- Proof of authenticity, which is usually a digital signature.

The holder of the IDC-ID is able to generate **verifiable presentations** of one or more IDC-ID in the way that the authenticity of the claim can still be verified (e.g., selective disclosure)

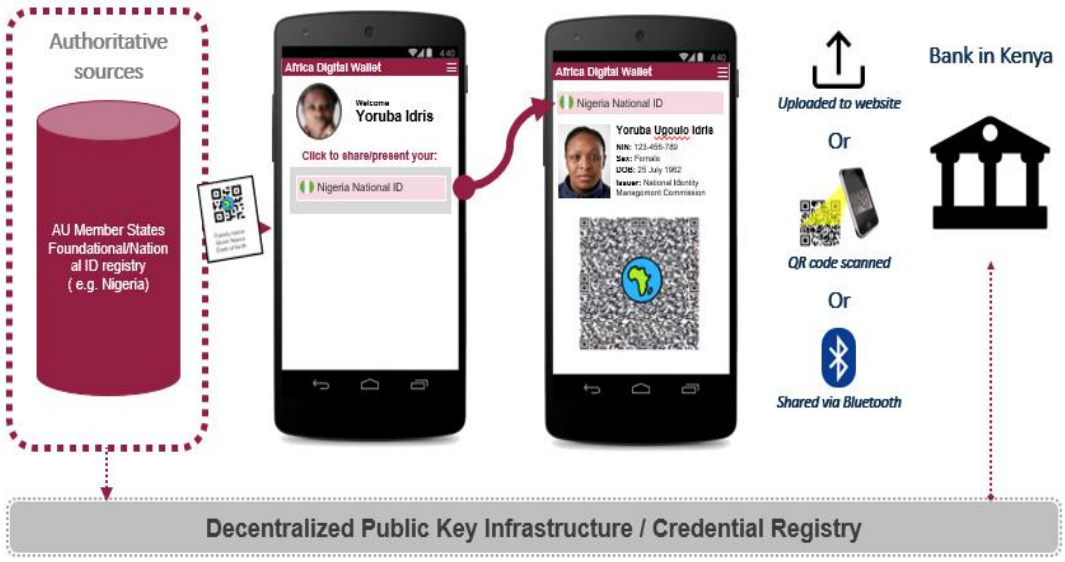
3.4. **Potential Authentication options**

Several architectural approaches can be adopted to enable the holder of IDC-ID to be authenticated at a given level of assurance. The following options can co-exist and be implemented at different levels of cooperation (e.g., among specific sectoral actors or at the REC level).
Depending on availability of other technologies with proven implementation practices, additional options may be explored.

3.4.1. Option 1 - Personal digital wallets

This option provides individuals and businesses with a personal digital wallet containing verifiable proof of legal identity attributes that can be used to prove one's identity or share specific facts with a service provider. This architecture option refers to W3C Verifiable Credentials Use Cases.[39]

Figure 2 – Overview of Option 1 - Personal Digital Wallets



Authentication process

1. Individual selects an **identity wallet provider** to store his/her IDC and an onboarding process is necessary.

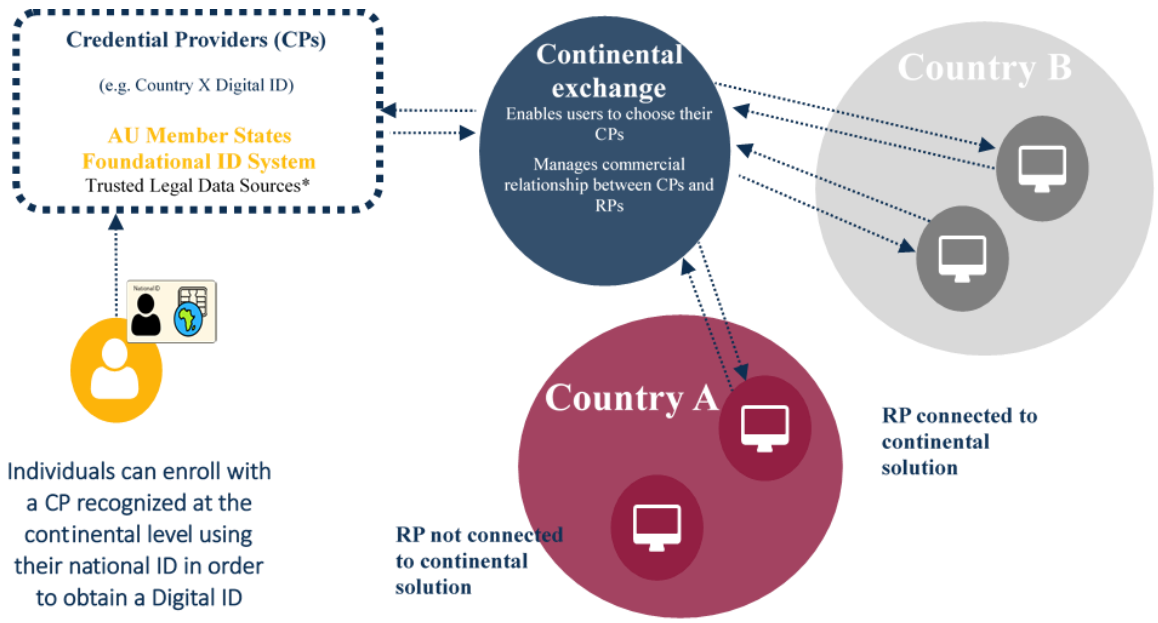
[39] W3C (2019) *Verifiable Credentials Use cases*, see: https://www.w3.org/TR/vc-use-cases/.

2. The individual receives a verifiable IDC (e.g., ID, proof of address) from the authoritative source issuers and stores it in a **digital wallet.**
3. At the same time of the issuance, the authority records a digital print of the claim in a **decentralised public key infrastructure, taking into account citizens' privacy**.
4. The individuals can present to a service provider (e.g., an insurance) a claim such as a **proof of address,** using his/her wallet (by QR code, Bluetooth, NFC).
5. The service provider can **verify** in the decentralised public key infrastructure that the claim is authentic and has been issued by a recognized authority.

3.4.2. Option 2 - Continental Digital ID federation

Under this model, each African resident would be able to onboard with a continental-level credential provider of their choice.

Figure 3 – Overview of Option 2 – Continental Digital ID federation



* *Member States will decide what trusted data sources entail their foundational ID systems*

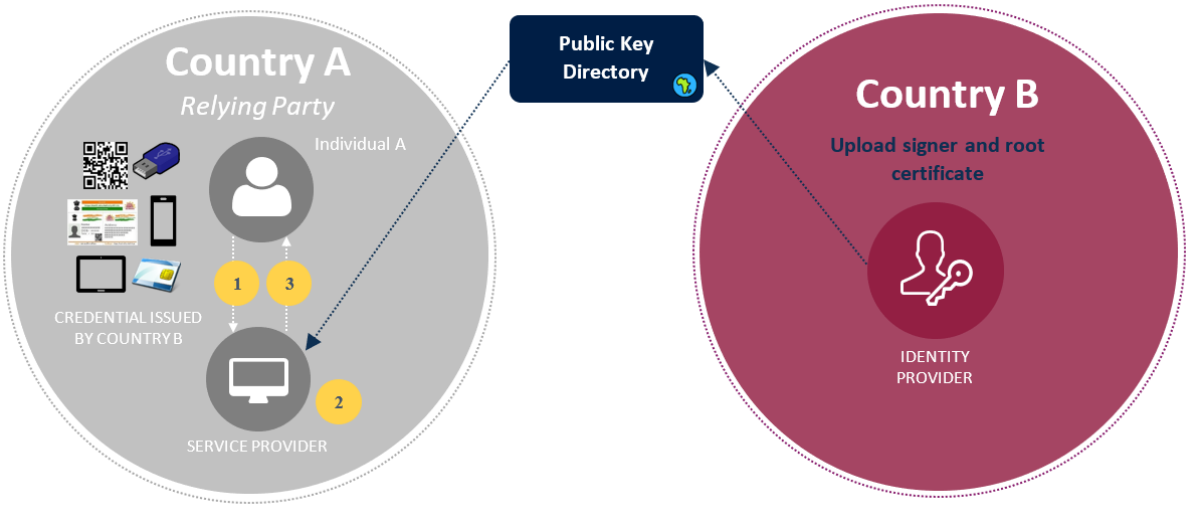
Authentication process

1. A **continental federation of ID credential providers is established**: telecom operators, banks, governments, etc., can provide authentication services.
2. A **continental exchange** is created, providing a single point of contact for all the participating credential providers and relying parties that want to authenticate individuals.
3. Individuals can use their IDC issued by an authoritative source (e.g., legal identification system) to **onboard** to the credential provider of their choice. The credential provider can verify the authenticity of the IDC.
4. Upon successful verification, the credential provider issues **an authentication means** to the individual.
5. The individual can use his or her authentication means to **access online and in-person services** that are connected to the continental exchange.

3.4.3. Option 3 - Digitally Signed credentials

This model enables authentication by verifying the digitally signed legal identity data on a credential with a public key, as well as an additional means to share the holder's picture.

Figure 4 – Overview of Option 3 - Digitally signed credentials



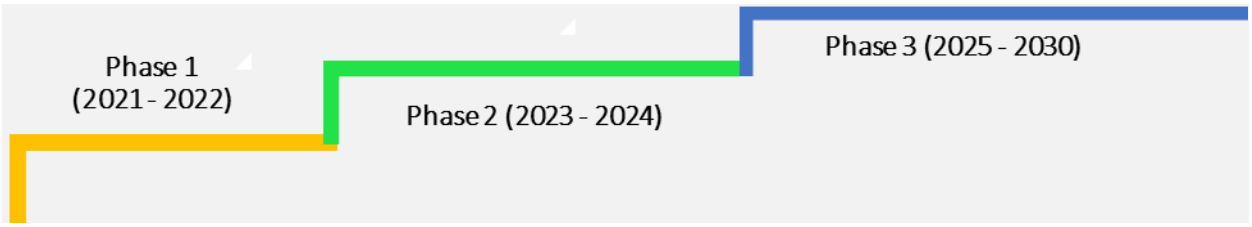
Authentication process

1. Countries agree on a **standard (e.g., a QR code) and** authoritative sources cryptographically **sign credentials** (via a private key).
2. Authoritative sources share their public key in a **Public Key Directory** (PKD) whose governance will be endorsed by AU Member States and managed at the continental level.
3. Countries create a separate service enabling to share a copy of the picture of the IDC-ID holder accessible via secure API in order to authenticate the holder. To work offline, it is also possible for a group of countries (e.g., RECs) to agree on the issuance of a physical credential containing a picture of the holder.[40]
4. Countries authoritative sources issue **standardised forms of IDC** to individuals.
5. A **verification software** (app or website) is created to enable service providers to verify the authenticity and integrity of the signature on the IDC.
6. Individuals can use their IDC to get their legal identity digitally verified by public or private relying parties in their country or abroad and **access services**.
7. Each Member State will be expected to maintain the private keys, root certificates and hashing algorithms in secure storage such as Hardware Security Modules (HSMs) for encryption and integrity checking.

[40] The issuance of physical credentials comes at an additional cost. Participating Member States would have to discuss further the financing of such solution in order not to create barriers to access.

4. High-level roadmap for implementation

To accelerate the path towards achieving the ambitious objectives of this Framework, AU Member States should increase their collaboration to refine the details of the technical and reference framework, common standards, and processes.
The proposition is to divide the implementation of the Framework in three phases, as shown in the diagram below: hope



1. Phase I: Adoption of the Framework and development of an enabling legislative framework;
2. Phase II: Implementation of the Framework and adoption of technical specifications for the IDC-ID;
3. Phase III: The scale-up of the Framework to provide an infrastructure enabling more advanced use cases such as remote authentication.

For each phase, opportunities for consultation with AU Member States, civil society, and other stakeholders of the identity ecosystem will be planned to ensure that the Framework and implementation remain aligned with the needs of the individuals and local contexts. Key documentation will be published and ample time will be provided for contributions and consultations.

4.1. Phase 1: Adoption of the Framework and enabling environment

Submission of the draft Framework to the 4th ordinary session of the STC on communication and ICT for adoption and the endorsement by policy organs.
Following the endorsement of the present document, the details of the Trust Framework will be further specified and the following activities will be conducted notably:

- awareness creation
- feasibility study on the current landscape of the digital ID system in Africa
- establishment of a consultation framework for digital ecosystem actors aimed at safeguarding the interest of each actor
- development of harmonised legal and regulatory instruments
- definition of the rules for participation;
- establishment of the governance mechanisms and forum to share best practices throughout the implementation process;
-
- defining legal provisions that will need to be integrated in domestic legal environments of AU Member States in order to implement the Framework, including appropriate safeguards on cybersecurity and data protection
- ratification of the Malabo Convention on Cybersecurity and Personal Data Protection;
- adoption of the continental data policy framework;
- nomination of expert groups by AU Member States to define the interoperability and

technical requirements;

- establishment of an independent institutional structures at national level (data protection authorities; controller of certifying authorities; and computer incident response teams (CIRTs) and strengthen cooperation among national institutions
- ;
- develop capacity building initiatives;
- support the roll-out of digital infrastructure including f data centres at national, regional/continental- level that required to support and sustain the operationalization of the digital ID systems
- resource mobilisation.

In order to ensure the success of the Framework, a series of **use cases** representing a range of opportunities for the continent will be defined. A group of AU Member States can further collaborate to test and pilot specific use cases, along with additional stakeholders as needed.

An assessment of the **major costs and benefits** of the proposed framework and subsequent authentication options should be conducted in order to provide more visibility on the financing needs and inform AU Member States decision-making. It is currently expected that compliance with a harmonised standard to represent identity information will engender limited costs for AU Member States as it could be integrated as a technical requirement to existing digitalisation projects of Member States' foundational ID systems. However, the establishment of the authentication infrastructure is expected to generate additional costs and depending on the types of stakeholders involved, require the definition of business models. For this phase, a detailed impact assessment will have to be performed in order to ensure that the authentication options proposed remain inclusive.

In parallel, AU Member States commit to:

- Develop and implement harmonized enabling legal and regulatory frameworks that build trust in digital foundational ID systems;
- Develop harmonized personal data legislation and regulation that empower individuals, while maintaining data sovereignty;
- rollout digital infrastructure including data infrastructure (national data centres) which is the base for rolling out the digital ID system
- ratify of the *AU Convention on Cyber Security and Personal Data Protection (if not done so far)*and expedite its entry into force and work to accelerate the establishment of data protection authorities for oversight in participating countries;
- Develop of the national cybersecurity strategy and establish of computer incident response teams (CIRTs) to mitigate risks and threats related to cyberattacks, data robbery and mishandling of sensitive information
- adopting the AU continental data policy framework; which calls for digital ID systems to be constructed and implemented cohesively in line with this overarching data governance framework that ensures that the combination and repurposing of public administrative data entailed by digital identification systems is done with appropriate safeguards. These should empower the individuals and protect online privacy as a fundamental right (to include user choice and control, informed/meaningful consent, data sovereignty/ownership, etc.);

- launching and/or scaling up efforts to strengthen foundational ID systems, and to ensure that they are inclusive and trusted, in line with relevant norms and initiatives such as the African Programme for Accelerated Improvement of Civil Registration and Vital Statistics Systems (APAI-CRVS) and the *Principles on Identification for Sustainable Development*.
  This phase will be finalised with the adoption of the completed version of the Framework by AU Member States.

4.2. **Phase 2: Implementation of the framework and adoption of technical specifications for the IDC-ID**

The second phase will consist of establishing the Trust Framework governance and cooperation mechanisms, and delivering the **technical specification** for the introduction of the IDC-ID. This will include, among other things:

- Develop minimum standards and norms for the interoperability
- attributing profiles for the minimum dataset (data formats) and associated metadata;
- presentation format (e.g., 2d barcodes, W3C verifiable credentials);
- level of assurance (as a reference point for interoperability);
- cryptography elements for data signing and encryption; and
- verification protocols for online and offline use cases.

Subsequently, a sample **implementation** (app or website) for basic verification of the IDC-ID can be developed by a group of AU Member States to test the interoperability of the credential and already support verifiable proofs of legal identity. The implementation will rely on the principle of privacy and security-by-design.
Participating entities will need to agree on the definition of **alternatives solutions to obtain an IDC-ID** for people that are currently excluded from any foundational ID system.
Additionally, a **mapping of other ongoing African Union initiatives** will be performed to build on the proposed framework (e.g., African Continental Qualifications Framework).
Phase 2 will then be concluded with the definition of a clear **action plan for the definition of the authentication infrastructure** as part of Phase 3.

4.3. **Phase 3: Development of the infrastructure to enable remote authentication**

Phase 3 will start implementing the Trust Framework defined as part of Phase 2.
In this phase, the layer that represents the issuance of the IDC-ID will be scaled up and expanded to implement an infrastructure that enables more advanced use cases such as remote authentication. This authentication layer will enable individuals to prove their identity digitally by exercising control of one or more authentication factors (e.g., a biometric or PIN code) bound to their previously verified legal identity, the IDC-ID.
Several technical options are available to AU Member States to implement this layer, including, for example, a federation of identity providers providing authentication mechanisms to the holders of the IDC-ID, or the development of digital ID wallet

solutions or any other models enabling interoperability. Each of these implementations can offer a data minimisation option and selective disclosure services for specific use cases (for example by only sharing the relevant data points from an ID card and credit report to obtain a loan, seek social or health benefit, obtain a pension benefit), where authentication is legally required, or anonymising the IDC-ID minimum dataset (e.g., name, date of birth) into a proof of majority (+18y or +21y or a yes/no response).

AU Member States will also be able to seek further discussion and agreement on how to establish this authentication layer infrastructure and partner with RECs and other continental initiatives that are already investigating the introduction of digital ID interoperable solutions to access services remotely. Indeed, Member States and organisations will be able to leverage the standard-based common representation of identity information in a trusted and secure digital format and build additional services on top of it.

AU Member States will continue collaboration to strengthen the Trust Framework and governance and cooperation mechanisms following agreement on the additional infrastructures, following:

- **coordination with other initiatives** aiming at establishing interoperability at a continental level (e.g., SATA and RECs); and
- **agreement on the best architectural option** (e.g., federation, digital wallets, etc.) to develop the remote authentication function that would build on the IDC-ID.

Phase 3 will be concluded with a clear action plan on the implementation of the authentication layer, as per the architectural option to be agreed among AU Member States and organisations.

5. High level Assumptions, Challenges and Risks

5.1. Assumptions

Member States will adopt the framework, collaborate, commit to implement, and make necessary and required legal and regulatory reforms.

5.2. General challenges and proposed high level mitigations

The below table summarises the general challenges and proposed mitigation mechanisms.

#	Challenges	Proposed mitigations
1.	Exclusion, weak security and erosion of personal data protection.	Apply the Principles defined in the framework (3.1) and strengthen the security and data protection legal frameworks and infrastructure

		in AU Member States.
2	Reluctance of AU Member States to adopt and implement the framework.	Raise awareness about benefits of interoperability framework at the domestic and continental levels and strengthen foundational ID systems.
3	Lack of technical and financial capability at AU Member States.	Enhance capacity and promote peer-to-peer knowledge exchanges among AU Member States, as well as consider cost effectiveness of technological solutions to be agreed on in Phases 2 and 3.
4	Inadequate data centres at the national/regional /continent levels.	Build national/regional/national data centres and promote their usage in Africa.

5.3. **Risks and proposed mitigations**

The below table summarises the risks and proposed mitigation mechanisms

9.	**1**	10. Absence of proper definition of common standard and lack of understanding by AU Member States and failure to follow and adopt common standards.	11. Definition of standards and communication of same to AU Member States during implementation, and regular monitoring by a trusted and enabled Pan-African body that is supported and endorsed by all Member States of the same to ensure adherence to standards. 12. Focused discussions and workshops with stakeholders to ensure clear definition of the standards for the chosen implementation strategy 13. Benchmarking the standard-based implementation strategy of AU Member States against similar, established standard-based national foundational ID programs across AU Member States.
14.	**2**	15. Low levels of trust between national authorities with heterogeneous enforcement capacities lead to a slow uptake of the framework at a large continental scale. In addition, Member States' unwillingness to accept a supranational supervisory body, slow down the implementation of the Trust Framework.	16. The framework should target harmonisation and mutual recognition as a long-term objective but remain open for flexible and agile solutions to be developed, which could create shared audit mechanisms between willing countries to establish trust among themselves while remaining sovereign – through the unilateral recognition of issued trust certificates.
17.	**3**	18. The solution, benefits, and options are not adapted well to the local environment or information is badly disseminated and the persons are not using the solution leading to poor uptake and ultimately high costs with little benefit.	19. Develop strong user-centric design structures to identify solutions that are easy to use and accessible to all. 20. Develop strong dissemination mechanisms across AU Member States that incorporates all like-minded local actors. 21.
22.	**4**	23. Member States will decide on the appropriate technology during implementation phase, however if they opt for PKI technology, absence of continental level certifying institution and lack of inadequate governance the cryptographic requirements for the digital signature may prove to be a hindrance in the set-up of interoperability system.	25. Creation of a legal framework enabling the establishment of a continental level coordinating institution that is supported by an equitable governance structure accounting for the sovereignty of each Member State for implementation and management of digital signatures, its issuance, revocation and timely replacement and updating. 26. Creation of a detailed and dynamic organisation structure to enable governance of digital signature/ PKI infrastructure across the implementation and the operations phase.

		24.	
27.	**5**	28. Due to incorrect and incomplete data, the design and implementation strategy of some of the interoperability components like digital signatures may be impacted. Delay in sharing of data and relevant information of the citizen or resident could also impact the timelines of the project.	29. Holding meetings with governments agencies for data gathering pertaining to implementation in the information gaps by leveraging the experience of the experts through peer-to-peer learning to encourage collaboration and regional and continental ownership. Monitoring of project timelines and milestones to prevent delays. It is also imperative to have a detailed and comprehensive implementation schedule which has been agreed upon by the AU Member States and key stakeholders.
30.	**6**	31. Absence of clearly defined change management guidelines to ensure that the Framework remains aligned with current practices, needs, and technological development.	32. Putting in place a robust and well-defined change management process as part of the governance framework.
33.	**7**	34. Member States will decide on the appropriate technology during implementation phase, however if they opt for PKI technology, certifying agencies in Africa may not reach a consensus regarding the management of PKI on the level of continent wide roll out. Secondly, there may not be consensus on setting up of digital signature exchange.	35. AU Member States either set up a new certifying institution for the management of PKI at the continent level or endorse a mechanism to bring the existing agencies on a common platform.
36.	**8**	37. Not having the necessary minimum legal enabling environment in place at the national and regional level.	38. AU Member States to speed up the implementation of the required harmonised legal and regulatory frameworks

39. **ANNEX**

39.1. **Working definitions**

Attribute is a named quality or characteristic inherent in or ascribed to someone or something (*adapted from NIST 800-63:2017*). In ID systems, common identity attributes include name, age, sex, place of birth, address, fingerprints, photo, signature, identity number, etc.

Authentication is the process of establishing confidence that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more “factors” to “assert” their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or is (e.g., their fingerprints) (*adapted from NIST 800-63:2017 and OWI 2017*).

Authorisation is the process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity (*Nyst,* et al*. 2016*).

Authoritative source is an authoritative source of identity information is a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or have conflicting data, the data within the authoritative data source is considered the most accurate (*FICAM, undated*).

Claim is a qualification, achievement, quality, or piece of information about a subject's background such as a name, government ID, home address, or university degree (*adapted from W3C*).

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Credential is a document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. In the case of this Framework, the credential is a verifiable claim called IDC-ID.

Data controller means any natural or legal person, public or private, any other organisation or association which alone or jointly with others, decides to collect and process personal data and determines the purposes.

Data protection regulates how data is used or processed and by whom, and it ensures citizens have rights over their data. It is particularly important in ensuring digital dignity, as it can directly address the inherent power imbalance between ‘data subjects’ and the institutions or people who collected data.

Data protection authority (DPAs) is an independent public authority that monitors and supervises, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints that may have breached the law.

Data sovereignty in this framework refers to personal data (including sensitive data) related to digital identification systems in an AU Member State must be collected, stored and processed (i) in facilities owned or controlled by and (ii) under the applicable law of the AU Member State.

Data subject means any natural person that is the subject of personal data processing.

Digital dignity (in the digital ID context) means that the human identity behind the digital ID has privacy and their data is protected.

Digital identification (ID) system is an identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication (*adapted from ID4D Public-Private Cooperation report*).

Digital ID is a set of electronically captured and stored attributes and/or credentials that uniquely identify a person (*adapted from Harbitz & Kentala 2013 and ID4D Technology Landscape report*).

Digital signature is an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection (*NIST 800-63:2017*).

Digital stack, in the context of digital technologies, is a collection of independent software components or infrastructure that work together to support the execution of a use case.

Foundational ID system is an identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity in order to access public and private services such as education, healthcare, social protection and financial services, etc. (*adapted from Gelb & Clark 2013a and various ID4D publications*). For the purposes of this Framework, AU Member States will decide which trusted data sources entail their foundational ID systems.

Functional ID system is an identification system created to manage identification, authentication, and authorisation for a particular service or transaction such as such as voting, tax administration, social programs and transfers, financial services, and more. Functional identity credentials—such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver's licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system (a*dapted from Gelb & Clark 2013a and various ID4D publications*).

Harmonisation is ensuring uniformity in the systems through the use of minimum standards to facilitate interoperability and legal and trust frameworks (e.g., for levels of assurance) to set rules and build confidence in respective systems.

ID is an acronym for identity credential or identity document in some areas.

Identification (ID) system is the databases, processes, technology, infrastructure, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose (*adapted from the Principles on Identification*).
Identification is the process of establishing, determining, or recognizing a person's identity. (*adapted from ISO/IEC 24760-1:2011 and ITU-T X.1252*).
Identity is the relative social coordinates which distinguish one individual from another. Identity can change depending on the actors or the setting in which individuals find themselves and is therefore neither fixed nor absolute.
Identity provider is an authoritative entity— e.g., a government agency or private firm—that issues and manages legal identities, credentials, and authentication processes throughout the identity lifecycle (*ID4D Public-Private Cooperation paper*).
Interoperability is the ability of different function units – e.g., systems, databases, devices, or applications – to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units (*adapted from ISO/IEC 2382:2015*).
Level of assurance (LOA) is the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity (*ID4D Public-Private Cooperation*). The overall level of assurance is a function of the degree of confidence that the applicant's claimed identity is their real identity (the identity assurance level or IAL), the strength of the authentication process (authentication assurance level or AAL), and—if using a federated identity—the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (*adapted from NIST 800-63:2017*).
Open standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. "Open Standards" facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (*adopted from ITU-T*).
Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.
Privacy- and security-by-design means proactively embedding privacy and security mechanisms into the design and operation of products and services both non-IT and IT systems, networked infrastructure, and business practices. This requires that privacy and security governance is considered throughout the whole engineering process and product lifecycle.
Data Protection Impact Assessment (DPIA) is a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the data protection laws and regulations.
Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means such as the

collection, recording, organisation, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of personal data**.**

Proof of legal identity is a credential, such as a birth certificate, identity card or digital ID credential, that is recognised as proof of legal identity under national law and in accordance with emerging international norms and principles (*United Nations Legal Identity Expert Group Operational Definition of Legal Identity*).

Relying party (RP) is an entity that relies upon the credentials and authentication mechanisms provided by an ID system, typically to process a transaction or grant access to information or a to system (*adapted from NIST 800-63:2017*).

Trust Framework refers to business, technical, operational, and legal requirements for the identity system to foster interoperability between the various participating parties.

Verifiable presentation is a tamper-evident presentation (data derived from one or more verifiable credentials) encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification, e.g., selective disclosure approaches that synthesize data and do not transmit the original verifiable credentials (*definition adapted from W3C*).

Verification is defined as the process of verifying specific identity attributes or determining the authenticity of credentials in order to facilitate authorisation for a particular service.

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

P. O. Box 3243, Addis Ababa, Ethiopia Tel.: (251-11) 5182402 Fax: (251-11) 5182400
Website: www.au.int

Department of Infrastructure and Energy
Information Society Division

DRAFT CONTINENTAL DATA POLICY FRAMEWORK

September 2021

Executive Summary

Data is increasingly recognised as a strategic asset, integral to policy-making, private and public sector innovation and performance management, and creating new entrepreneurial opportunities for businesses and individuals. When applied to government services, emerging technologies can generate massive amounts of digital data and significantly contribute to social progress and economic growth. The central role of data requires a high-level and strategic policy perspective that can balance multiple policy objectives - from unleashing the economic and social potential of data to the prevention of harms associated with mass collection and processing of personal data.

The purpose of this document is to provide the policy framework for African countries to maximise the benefits of a data-driven economy through creating an enabling policy environment for the private and public investments necessary to support data-driven value creation and innovation. This enabling environment refers both to the collaboration between in-country sectors, institutions and stakeholders, an alignment of their development priorities, and the harmonisation of policy across the continent in a manner that provides the scale and scope required to create globally competitive markets.

From a policy perspective, the approach adopted is people-centred, locating them in relation to the role of data in contemporary economy and society by identifying the elements and linkages in what can be called the “data ecosystem” in order to identify the exact points of policy intervention. This allows for a systemic assessment of the interrelated challenges arising from global developments that impact on emerging national data economies and those arising within the context of nascent data driven economic activity, uneven institutional endowments, and human development in many African countries. This enables the design of a contextually grounded but forward-looking data policy framework that uses economic regulation to guide policy makers in realising opportunities of data-driven value creation. The framework points to ways in which opportunities can be realised and how associated risks could be mitigated by creating an enabling and trusted environment.

Building a positive data economy national and regional will require unprecedented levels of collaboration between stakeholders to disrupt the economic, political, and policy pressures already being felt from the global data economy. In order to ensure equitable and safe access to data for innovation and competition, Member States should establish a unified legal approach that is clear, unambiguous and offers protection and obligations across the continent. Where necessary existing legal instruments and institutions should be revisited to ensure that they are not in conflict with one another and that they offer complementary levels of protection and obligations.

A comprehensive data strategy will necessarily include the harmonisation between competition, trade, and taxation policies and laws both at the national and regional levels. This is so an optimised data ecosystem for Africa balances revenue mobilisation and the need to avoid distortions to local markets and the global tax system. Intellectual property laws should also be revised to clarify that they do not generally impede the flow of data or data protection. At the same time, governments need to develop transversal digital policies and strategies to coordinate activities across the public sector and between the public and private sectors to meet national objectives.

While there are multiple, competing definitions of data, common to all is the recognition that there are many different types of data. There are also numerous ways that data can be categorised that affect the appropriate policy and regulation of that category in order to mitigate any potential risk associate with the processing, transfer or storage of it. A primary distinction is that between personal data and non-personal data, with data protection referring to ensuring the privacy of data subjects. Data categorisation guidelines should be one of the first actions of the data information regulator, a key institution for the development of an

integrated national data system, which should be established in partnership with all relevant stakeholders. Essential to the development of an enabling environment for the data economy is ensuring the necessary foundational digital infrastructure, and the human resources necessary to develop data as a strategic asset. Due consideration needs to be given to developing robust Digital ID systems for the delivery of public and private value to citizens and consumers.

As the framework also emphasises, this can only be properly achieved through instilling a culture of trust in the data ecosystem. This is done through the establishment of safe and secure data systems based on effective cybersecurity and data protection rules and practices, and ethical codes of conduct for those who set data policy, implement it and those who use data – whether in the public, private or other sectors. This is not sufficient however. Trust in data governance and a national data system is established through legitimacy. This includes systems and standards that guarantee public and private sector compliance, government itself adhering to personal data protection rules, and government sharing public data.

The framework instils the importance of collaborative and evidence-based policy processes for the domestication of the policy proposed. The governance and institutional arrangements should assign clear roles to the government as policy maker, and independent, agile and capacitated regulators to implement policy and effectively regulate the data economy to ensure that fair competition produces positive consumer welfare outcomes. The creation of data and information regulators, to promote and safeguard the rights of citizens and their participation and fair representation in the data economy and society, will need to be a priority for those countries that have not yet established these. Coordination with other regulators to achieve this will be essential. The legal ecosystem must be harmonised and rebalanced.

Access to data is a prerequisite for value creation, entrepreneurialism and innovation. When data are of poor quality or not interoperable, they limit the capacity of firms and the public sector to engage in the sharing and analytics that can provide economic and social value to data. These processing frameworks should align with the following principles: consent and legitimacy; limitations on collection; purpose specification; use limitation; data quality; security safeguards; openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity. Security models also need to be transversal, with specific emphasis on cloud storage and processing of sensitive/proprietary data, API management, and support of equitable data economies

Attention needs to be paid to access to quality, interoperable and reliable data – primarily from the state, but also from the private and other sectors – with a reinvigoration of the principles of open governance across the continent. Capacity-building should be a key national and regional priority, and resources will need to be allocated in this regard in the areas of data protection, cybersecurity and institutional data governance in relevant agencies. Skills and an understanding of the data ecosystem will also need to be built in state institutions, amongst other sectors and communities.

The framework is guided by the broad principles of transparency, accountability of institutions and actors, inclusion of stakeholders, equity among citizens and fair competition amongst market players. The principles guiding the framework include trust, accessibility, interoperability, security, quality and integrity, representivity and non-discrimination.

As the framework emphasises, transversal collaboration needs to be underpinned with mechanisms to stimulate demand for data, which includes incentivising innovative data communities, and, on the supply-side, ensuring the quality, interoperability, and relevance of data in both the public and private sectors, and civil society.

As the framework suggests, there are several regional processes, mechanisms and instruments that can and should be leveraged in the continent's efforts to develop a cohesive data policy

framework. These include the African Continental Free Trade Agreement (AfCFTA), which provides an opportunity for co-operation on a number of important aspects of the policy framework. Collaboration between national and regional stakeholders is also necessary for African countries to become more competitive in global policy setting forums where regulations for the global data economy are set, and where African states have largely been "standard takers".

It is recognised that different African states have different economic, technical, and digital capabilities, and the recommendations and actions need to be read in this light. It is nevertheless envisaged that the different demands of building a data ecosystem will be progressively realised by countries. At the same time, there are several areas that can be attended to independently of economic or technical capabilities, including establishing regulatory independence, promoting a culture of trust and ethics, building collaborate frameworks for relevant sectors, developing transparent, evidence-based and participatory policy and regulations, participating in collaborative regional processes and mechanisms, and ratifying the AU Convention on Cybersecurity and Personal Data Protection.

The Framework presents a set of detailed recommendations and arising actions to guide member states through the formulations of policy in their domestic context as well as recommendations to strengthen cooperation among countries and promote intra-Africa flows of data. The main high-level overarching recommendations are included here. It is recommended that Member States:

- ❖ cooperatively enable data to flow on the continent while safeguarding human rights, data protection , upholding security and ensuring equitable sharing of the benefits.
- ❖ cooperate to create the necessary data capabilities to take advantage of data-reliant technologies and services, including the capacity to govern data so that it benefits African countries and citizens and enables development;
- ❖ promote transversal data policy and agile regulation to navigate the emergence of new dynamic data-driven business models that can foster intra-Africa digital trade and data-enabled entrepreneurship;
- ❖ create co-jurisdictional frameworks for the coordination of autonomous competition, sector, and data regulators to regulate the data society and economy effectively, formulate, implement, and review data policy in a dynamic, forward looking and experimental way;
- ❖ Develop national legislations on personal data protection and adequate regulations, particularly around data governance and digital platforms, to ensure that trust is preserved in the digital environment.
- ❖ establish or maintain independent, well-resourced and effective Data Protection Authorities , strengthen cooperation with DPAs from members of the African Union and develop mechanisms at the continental level to develop and share regulatory practices and support institutional development to ensure high level of protection of personal data ;
- ❖ promote interoperability, data sharing and responsiveness to data demand through setting of open data standards in data creation conform to the general principles of anonymity, privacy, security and any sector-specific data considerations to facilitate non-personal data and certain categories of personal data are accessible to African researchers, innovators and entrepreneurs;

- ❖ promote data portability so that data subjects are not locked into a single provider and in so doing promote competition, consumer choice and to enable gig workers to move between platforms;
- ❖ improve unevenly developed infrastructure across the continent, leveraging existing REC regional efforts to support efficient broadband network coverage, reliable energy supply, and foundational digital (data) infrastructure and systems (FDI) (digital identity (Digital ID), interoperable trustworthy payments, cloud and data infrastructure, and open data sharing systems, for cross border digital trade, e-commerce;
- ❖ establish an integrated national data system to enable data driven public and private value creation, operating on the basis of harmonised governance frameworks that facilitate the flow of data necessary for a vibrant data economy, but with sufficient safeguards to be trusted, safe and secure.
- ❖ govern the integrated national data system according to the principles of access, availability, openness (where anonymity can be preserved) interoperability, safety, security, quality, integrity;
- ❖ integrate sector specific and specialists data codes or guidelines into national and continental data governance regimes;
- ❖ who have not yet ratified the AU Convention on Cyber Security and Personal Data Protection do so as soon as possible, to serve as the foundational step for the harmonisation of data processing; and

- ❖ in the forthcoming negotiations on Trade in Services and E-commerce protocols, as well as the Competition and Intellectual Property protocols, in the African Continental Free Trade Area provide guidelines to promote access to data to support local innovation, entrepreneurialism and for pro-competitive purposes.
- ❖ prioritize politically neutral partnerships that take into account individual sovereignty and national ownership to avoid foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States

- ❖ promote research, development and innovation in various data based areas including, Big Data Analytics, Artificial Intelligence, Quantum Computing as well as Blockchain

It is further recommended that The African Union Commission, RECs and Regional Institutions:

- ❖ facilitate collaboration between the various entities dealing with data across the continent through the establishment of a consultation framework within the digital ecosystem community to safeguard the interest of each actor.
- ❖ promote and facilitate data flows within and among AU Member States by developing a Cross Border Data Flows Mechanism that takes into account the different levels of digital readiness, data maturity as well as legal and regulatory environments of countries ;

- facilitate data circulation across sectors and cross borders by developing a Common Data Categorisation and Sharing Framework that takes into account the broad types of data and the associated levels of privacy and security;

- Work in in close collaboration with national authorities in charge of personal data protection of AU members, with support of the African Network of Authorities (RAPDP), to establish a coordination mechanism & body that oversees the transfer of personal data within continent and ensures compliance with existing laws and rules governing data and information security at national level.

- Establish or empower a mechanism within the African Union for centralising and empowering regional engagements on data standards.

- establish mechanisms and institutions , or empower existing ones, within the African Union to build capacity and render technical assistance to AU Member States for the domestication of this data policy framework; and

- Support the development of regional and continental data infrastructure to host advanced data-driven technologies (such as Big Data, Machine learning and Artificial Intelligence) and the necessary enabling environment and data sharing mechanism to ensure the circulation across the continent;

- Work towards building a secure and resilient cyberspace on the continent that offers new economic opportunities through the development of an AU Cyber Security Strategy and establishment of Operational Cybersecurity Centres to mitigate risks and threats related to cyberattacks, data breaches and misuse use sensitive information.

- establish an Annual Data Innovation Forum for Africa to raise awareness amongst policy makers about the power of data as the engine of a digital economy and society, so as to facilitate exchanges among countries and enable knowledge sharing on data value-creation and innovation and the implications of data usage on peoples' privacy and security .

- Strengthen links with other regions and coordinate Africa common positions on data related international negotiations to ensure equal opportunities in global digital economy;

- develop an implementation plan that takes into consideration digital sovereignty of states as well as the different levels of development, vulnerability of populations and digitization within AU Member States namely aspects related to ICT infrastructure gap and lack of cybersecurity policies and legislations .

-

Table of Contents

1. Introduction

Data are at the core of the digital transformation taking place at an unprecedented pace and scale globally. The deployment of data-driven technologies to transform most aspects of our daily lives and work into quantifiable data that can be tracked, monitored, analysed and monetised has become such a phenomenon that the term ‘datafication’ has been coined to describe it.

These processes - which have accelerated during what has been referred to as the first ‘data-driven pandemic' - can turn public and private organisations into data-driven enterprises, improving information flows and efficiencies, and creating more competitive economies. Enhanced information flows under the right conditions can also reduce information asymmetries between governments and citizens, ultimately strengthening good governance. Some of these processes have been incremental and some disruptive, but they have all been highly uneven. Data utilisation is one of the key drivers to accelerate the achievement of Agenda 2063 and the Sustainable Development Goals (SDGs), with the absence of good data being one of the primary challenges to assessing the progress being made to achieving the underlying targets. Specifically, improved integrated data systems directly contribute to achievement of several of the goals such as improved health, education systems identity systems but without direct policy intervention, the current uneven distribution of opportunities and harms arising from datafication between countries and within them will be exacerbated.

Whether African states can create the conditions for the harnessing of these processes of digitalisation and datafication to create added value, increase efficiency and productivity, improve social services and create new forms of work will depend on the policies adopted and implemented. This calls for a collaborative African response.

Maximising the benefits of a data-driven economy and minimising the risks are highly dependent on enabling policy and regulatory frameworks that increase legitimacy and public trust in the management of data. Data infrastructure that enables an integrated data system is a key strategic asset for countries, but the scale, extent and speed of change brought about by data-driven digital technologies make regulation complex and resource intensive. As emerging technologies become more central to the data economy, the diversity of stakeholders and plethora of platforms involved in its regulation also expand dramatically, making it increasingly difficult for policymakers to remain involved and informed (African Development Bank, 2019). Emerging advanced technologies like AI are likely to increasingly challenge the efficiency of traditionally disparate legislative approaches to law making.

Data are global in nature, meaning that on the one hand, regulations have cross-border implications, and that on the other, regulatory precedence is most often set by data-rich and data-intensive developed countries. Market pressure is also imposed by oligopoly firms, notably Facebook, Apple, Microsoft, Google, and Amazon (or FAGAM). The nature of data allows these firms trading in global data driven digital markets to leverage their competitive advantage in data and algorithms across the globe. This ultimately affects local competition and inhibits the global competitiveness of domestic data economy participants. There are therefore issues of intellectual property and data access, fair trade, competition and consumer rights that impact data policy in a global context and raises the need for global governance and collaboration.

These factors also highlight that much of what drives the development of the local data economy, has been outside of the control of African stakeholders, who have been largely ‘standard takers’ in global governance. They also underscore the need for collaboration and partnerships in many African data ecosystems, regardless of digital maturity and broader economic endowments.

This policy framework therefore presents opportunities for countries to ensure that laws proactively enable access to data for developmental, innovative and competitive purposes. At the same time, it demonstrates the need for these to be in harmony with one another to create the scale and scope in the market necessary for data-driven value creation and innovation which can catalyse the single digital market envisaged in the African Union Digital Transformation Strategy.

2. Mandate

The central role of data **requires a high-level and strategic policy perspective that is strongly rooted in the local context** and can balance multiple policy objectives. National data strategies and internationally interoperable approaches can help unleash the economic and social potential of data while preventing harms and mitigating risks (OECD, 2019).

This data policy framework derives from the Digital Transformation Strategy (DTS) 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.[41] 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 Data Policy Framework builds on existing instruments and initiatives such as the Digital Transformation Strategy for Africa 2020-2030 (DTS), the Africa Continental Free Trade Agreement (AfCFTA) , the Policy and Regulatory Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), Smart Africa Vision to Transform Africa into a Single Digital Market by 2030, the Free Movement of Persons (FMP), the Single African Air Transport Market (SAATM), The Single Electricity Market in Africa, the Interoperability framework on Digital ID, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the Declaration on Internet Governance and Development of Africa's Digital Economy of 2018, the Personal Data Protection Guidelines for Africa, regional model laws on data protection and cybersecurity and the African Union Charter on Human and People's Rights.

This Data Policy Framework sets out a common vision, principles, strategic priorities and key recommendations 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. The potential of data-driven solutions to overcome most of Africa's development challenges is made possible by Member States adopting a common data policy underpinned by a coherent governance approach. Furthermore, the development of integrated data systems is critical to optimise information flows and productivity gains from digitalisation and datafication.

This Data Policy Framework aims to strengthen and harmonise data governance frameworks in Africa and thereby create a shared data space and standards that regulate the intensifying production and use of data across the continent. This by creating a safe and trustworthy

[41] The Executive Council at the Thirty Six Ordinary Session held on 6-7 February 2020 endorsed the Digital Transformation Strategy for Africa (2020-2030), referenced in decision [EX.CL/Dec.1074 (XXXVI)], as the master plan that will guide the digital development Agenda of the continent, with Data as one of its cross-cutting theme and as a building block for the establishment of Africa digital economy and society. To enable the creation of Africa's digital economy and society, the Executive Council in its decision [EX.CL/Dec.1074 (XXXVI)], tasked the AU Commission to lead and coordinate the development of a continental framework on data policy and its submission to the STC-CICT 4 in 2021 for consideration and endorsement.

digital environment to boost the development of an inclusive and sustainable digital economy that fosters Intra-Africa Digital Trade in line with the ongoing regional economic integration initiatives under the AfCFTA.

Data use case for value creation
Data deserts in many African countries reflect the digital divide, as many people do not have access to the services and systems used to generate the data that are needed to train algorithms or to analyse for decision-making. User-generated data sets, such as social media updates and call direct records (CDR), are a major part of the data revolution, provided they are collected in a responsible manner. These data sets can be combined and repurposed with other data such as anonymised citizen data to reflect the lived experiences of millions of individuals and provide valuable information about many different vulnerable communities that can inform policy making, enhance interventions, and spur economic activity across various use cases. For example in Senegal big data was used to map CDR, mobility , and economics activity, in Kenya big data on M-Pesa mobile money transactions was used to create credit and savings products for subscribers and create credit profiles for small-holder farmers for input and harvest loans, a section of the economy that is typically not able to access formal banking facilities[42]

2.1 Vision

The Data Policy Framework envisions the transformative potential of data to empower African countries; improve people's lives; safeguard collective interests; protect (digital) rights; and drive equitable socio-economic development.

Practically the process seeks to translate this vision into a framework which will, when implemented:

- empower Africans to exercise their rights through the promotion of trusted, safe and secure data systems integrated on the basis of common standards and practices;
- create, coordinate and capacitate governance institutions to regulate, as necessary, the ever-changing data landscape and to increase the productive and innovative use of data to provide solutions and create new opportunities while mitigating risk.
- ensure that data can flow across borders as freely as possible, while achieving an equitable distribution of benefits and addressing risks related to human rights and national security.

2.2. Scope and objectives

Given that data now traverses every aspect of our daily lives, but under very different circumstances across the continent, the **framework provides principle-based guidance** to member states in their domestication of the continental data policy appropriate to their conditions and proposes a continental instrument or mechanism to integrate and coordinate continental efforts. The Africa Data Policy Framework aims to **strengthen national data systems** for effective use of data by creating an enabling environment that **stimulates innovation, entrepreneurialism to drive the development of data value-driven economies** and that facilitates the interoperability of systems and cross border data flows necessary for the realising of the African single digital market. Harmonised across the African markets this affords the regulatory certainty and the scale and scope conducive to investments required for data-driven public and private value creation with the associated distributional impacts and non-economic multipliers.

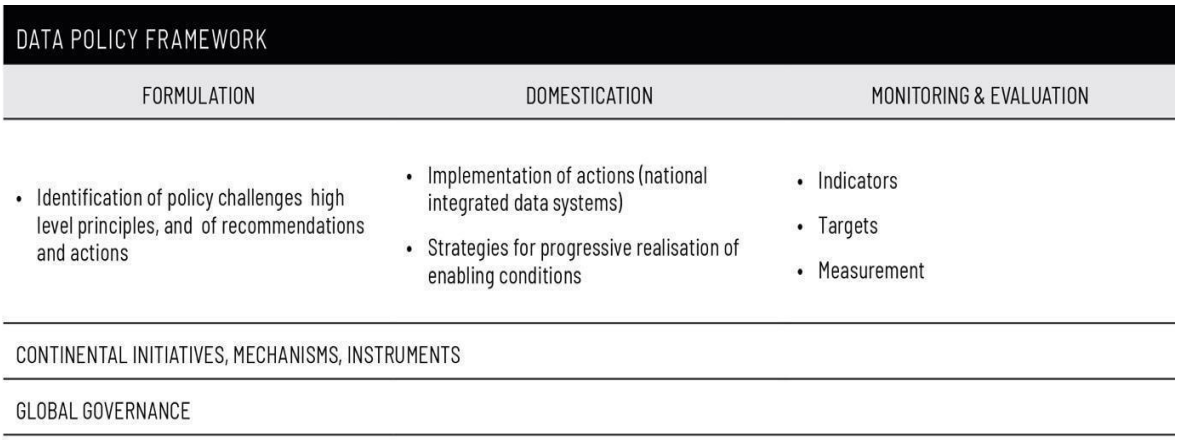
With regards to the scope of the framework, it is important to bear in mind that the policy is concerned with **data governance that includes personal, non-personal, industrial and public data**, not only personal data protection that has been the focus of attention internationally and on the continent in recent years.

[42] See https://www.developlocal.org/the-big-data-in-africa-report/

The specific and overreaching objectives of the African Data Policy Framework are to:

- enable states to cooperate on matters of data governance to achieve common objectives related to the sustainable development of their economies and societies;
- inform and support the domestication of continental policy by African countries;
- ensure that data can flow across borders as freely as possible, while promoting an equitable distribution of benefits and addressing risks related to human rights violations and other legitimate interests of states such as the fight against money laundering, tax evasion, online gambling, national security,.
- foster and facilitate cross border data flows and increase business opportunities while ensuring an adequate level of personal data and privacy;
- establish collaborative trust mechanisms to allow for data to circulate as freely as possible between Member States, while preserving the sovereignty of Member States and their ability to regulate the digital economy
- enable states, the private sector, civil society and intergovernmental organisations to coordinate their efforts on data issues across the continent to realise a single digital market and compete more effectively in the global economy;
- enable competitiveness in the global economy through close and sustainable cooperation by African states, the private sector and civil society through restructuring opportunities to optimise the benefits from datafication of the economy and society.
- ensure that data are used in a sustainable manner that benefits society as a whole and does not harm people's privacy, dignity and security;
- ensure that data are widely available within appropriate safeguards for both commercial and non-commercial use; and
- facilitate innovative ways to promote public benefits by using data in new ways that would enable the data in Africa to realise the value of data in public sector decision-making, planning, and monitoring and evaluation.

To enable the continental data policy to meet its envisioned objectives and reflect the interests of all stakeholders, the formulation of the **policy framework is informed by previous initiatives and documents** both from within and outside Africa. The process included an open public consultation. Inputs made through this online consultation and a public webinar contributed to the development of the draft policy framework.
The AUC coordinated the development of the continental Data Policy Framework in collaboration with Pan African organisations and AU specialised Agencies and Institutions namely: Regional Economic Communities, AUDA-NEPAD, Smart Africa Secretariat, African Development Bank , Africa Telecommunications Union (ATU) , the UN Economic Commission for Africa, International Telecommunication Union(ITU) , the UN Council on Trade and Development (UNCTAD), the World Bank as well as other partner institutions.



3. Rise of the data economy - need to re-think policy

A shift in approach to data regulation is required for countries to properly benefit from the emerging global data economy. This shift informs this framework. Key elements of this integrated approach to data policy formulation are outlined below.

3.1. Data as the basis for new social contract and innovation economy

As data in and of themselves have little value, it is only through the processing, transmission, storage and combination that value is added. In economic terms data can be understood as a public good in that it is inherently non-rivalrous (at the technical level, it is infinitely usable without detracting from another person's ability to use it). It is naturally non-excludable which means that there are no natural barriers to multiple people using the same data at once. Although there are attempts to render data excludable through technological and sometimes legal means, these are not inherently features of data. Attempts to limit access whether for purposes of commercialisation or security can be regulated to be non-excludable. For example data that are made open under an internationally recognised licence or public statistics can be regulated to be accessible like free to air public broadcasting, as classical public good.

Data also does not automatically generate value. Instead there are different uses of data and different methods to measure the economic and social value of data and data flows (OECD, 2019). In the economic sense, it is what firms do that leads to value creation both internally within the firm and externally across the extended-data network. Theoretically, this value can be quantified by assigning monetary value taking in consideration several cost and income-generating variables, such as how organisations charge for user-generated data, or reconciling data management costs such as collecting, maintaining and publishing data. Valuing data from a socio-economic benefits perspective – or non-market-based data value – arises when there are fundamental conditions or enablers that allow governments to deliver more effective public services, offer effective environmental stewardship, and when citizens live healthier and economically secure lives through leveraging data (World Bank, 2021). Example of public data value creation includes using data to inform resource allocation needs to enhance service delivery.

These characteristics of data have elsewhere been framed as the **potential of data to provide the basis of a new social contract** (World Bank, 2021). Arising policy directions from this approach emphasise the need open data, interoperability standards and data-sharing initiatives to harness the potential of data for driving development; ensuring a better distribution of the benefits of data; fostering trust through safeguards that protect people from the harm of data misuse; to create and maintain an integrated national data system that allows the flow of data among a wide array of users in a way that facilitates safe use and reuse of data.

Trust is central to a robust, flourishing data environment. Trust is often equated in the context of digital governance with technical security and the confidence in the technical system required for e-commerce to operate. While technical security may be a necessary condition for trust, it is not sufficient. Instead, trust-building permeates the entire data ecosystem, from the people-centred formulation of rights-preserving policies and regulations, to ensuring access to and use of data to enable more equitable inclusion in the data economy.
Although the harms associated with concentration of data and information and asymmetries of power are universal the impacts are uneven, both between and within countries. Creating policies that mitigate the differential risk for different categories of people, such as children, or categories of data in different sectors such as health data, or ensuring that the increasing centrality of data does not perpetuate historical injustices and structural inequalities will require far more granular and adaptive regulation. While a rights preserving data policy framework will be essential, the individualised notions of privacy, freedom of expression and access to information (first generation rights) in current data protection normative frameworks will not be sufficient to ensure more equitable and just outcomes. Second-generation social and economic rights are also relevant to several areas of data governance in relation to data availability, accessibility, usability, and integrity that require data governance to impact equitable inclusion. This highlights the need to move beyond only negative compliance regulation to positive enabling regulation that will create an environment for African states and citizens to participate effectively in the digital economy. Creating the conditions that allow for the necessary access to data while safeguarding rights will require building institutional capacity within the state and the capabilities to regulate agilely to harness the potential of data to address some of the continent's most intractable problems.
To do so, **policy makers need to balance some of the tensions in the valuing of data i**n order to optimise it for these purposes. The transformation of data into useful information to guide decision-making revolves around the data value chain where firms and certain public entities are adequately equipped with enabling frameworks to support a coherent data ecosystem. Generating value from data can enhance private interests, such as improving firm operational efficiency, increasing their customer base, and creating innovative products and services that benefit commercial activities and data subjects. For governments, public value from data is realised by ensuring that the socioeconomic benefits of data accrue to enabling the achievement of wider socio economic goals. While public and private data valuation have different intentions and outcomes, they are not mutually exclusive. In fact, market and non-market value should not be correlated with private sector and public sector. Non-market value could be linked to research or civil society too. The public sector can also create market value by opening certain data sets and establishing new revenue streams. There are also innovative interplays between public and private actors that can improve the overall data ecosystem to meet socio-economic development needs and enhanced welfare.
With the increasing complexity and adaptiveness of the global communications system, both newer and more traditional forms of governance are arguably proving incapable of providing adequate tools for the governance of global public goods such as data. From a policy point of view there is a growing distinction being drawn between data value-creation and the value-extracting features of existing data-intensive and platform-oriented industry behaviour and business models (Mazzucato et al., 2020). There has been little restraint either from competition or data regulators on the rise of monopolistic global platforms producing and extracting massive amounts of private data, which has been commodified with seemingly

little regard for the social and negative implications for the data subjects (Zuboff, 2018). This may require specific, and transversal regulatory responses in order to preserve the positive obligations of data governance.

3.2 Need for data governance - creating value, preventing harms

Data governance at a macro level emerges as an opportunity to use standards, rules, norms and principles as mechanisms for both mitigating against identified data risks and harms, while advancing data economy development and digital dividends.
Policy on data governance therefore has some practical mechanisms:

- Aligning the principles to underscore data governance as a normative function;
- Assigning roles and responsibilities for the implementation of policy at a macro and micro level;
- Identifying and ensuring legal and policy clarity for mechanisms for implementing data governance;
- Identifying and encouraging collaboration across vertical and horizontal stakeholder groups;
- balancing the need for a circulation of data to enhance value creation while creating economic incentives for investments in data infrastructure and services and so on; and
- establishing trust mechanisms to support data sharing under terms and conditions agreed by all parties on rules for data use and issues of liability (data accuracy for instance).

This simplification of data governance policy must then be contextualised within the challenges and opportunities described below. In so doing, governance priorities become:
Data definition - Providing specificity and detail on the types of data to be regulated, and to what extent, to ensure the maximisation of benefit for different role players in the implementation of data policy. This should be done cognisant of the value and nature and data.
Continental coordination - Providing mechanisms and priorities for coordination within the continent to strengthen Africa position within global governance and provide support for l domestication.
Domestic institutional capacity - Assigning obligations, responsibilities and powers for institutional actors at the national level that can help create a consistent domestic environment for data communities (public and private) to institute data activities.
Domestic collaboration - Ensuring policy alignment, identifying multi-stakeholder participants and advancing mechanisms for successful domestication.
Policy support - Providing implementable standards and solutions that focus on the achievement of healthy domestic data quality, control, access and interoperability, processing and protection, and security as the means for growing a data economy.
Clarity - Ensuring clarity, which facilitates compliance, does not have unintended restrictions, but can also serve as foundations for cross-border (and cross-silo) coordination.

4. Context

4.1. Overview of international regional policy and legislation trends

Many jurisdictions across the world do not have data policy, with about a third having no data legislation in place. UNCTAD found in 2020 that 66% of countries in the world have some sort of legislation, 10% have draft legislation, 19% have no legislation and 5% have no data legislation at all.

Globally, a number of instruments have emerged in this context such as the EU GDPR 2016/679, the APEC Privacy Framework and the Trans-Pacific Partnership (TPP) Agreement. These agreements take slightly different approaches to data protection and may serve as points of reference for Africa's concerted efforts at data protection.

The EU's GDPR 2016/6 is wide-ranging with an expansive definition of what personal data is. Its broad territorial scope applies within and outside the EU, contains serious penalties for subverting the regulation, requires considerable openness and transparency and, importantly, grants individuals substantial rights that can be enforced against businesses. This approach to data protection is centred around a human rights agenda in the digital ecosystem.

The APEC Privacy Framework, which has been applied by APEC member states since 2005, is made up of a set of principles, which are set up to ensure the free flow of information in support of economic development. APEC's framework takes a different approach to data protection by aligning the framework's mandate with the promotion of trade and investment. An important highlight of the framework is how it emphasises that privacy regulations must take into consideration the importance of business and commercial interests in addition to the cultures and other diversities of member states economies.

The Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) focuses on open trade and regional integration amongst member states. The agreement allows for the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the businesses but countries can require protection of data that is transferred

Outside of these multilateral agreements, the public goals of data protection most typically centre around protecting the privacy of individuals and communities; safeguarding valuable data from leaks, loss, and theft; and maintaining and increasing public, investor and customer confidence. In a bid to achieve these goals, many countries have included in their domestic laws potential barriers to data flow such as data localisation requirements and, in some instances, more stringent data processing and collection requirements. These may inadvertently retard or counteract the objects of more far-reaching regional policy frameworks.

In the evolution of domestic policies for the digital economy, several strategies have crystallised globally, such as the government-led approach (as championed by the EU), the private sector-led approach (as promoted in the United States), the top-down policy approach (exemplified by Singapore), and the bottom-up approach (for instance, in Hong Kong, China). These approaches have varying complementary effects on policy implementation, deployment, impact, innovation, agility and stability.

4.2 African policy and legislative context

In line with international precedents, most efforts in data regulation on the continent have focused on data protection, with the chief aim being to observe and safeguard internet user's privacy rights. While the use and processing of data is a cross-cutting concern, which impacts an array of traditionally siloed areas of policy, there are no examples of umbrella laws that regulate every aspect of data. Instead, data has been regulated across five branches of the law: data protection law, competition law, cyber security law, electronic communications and transactions law and intellectual property law, which potentially conflict in some instances and leave gaps in others.[43]

It is estimated that **32 of Africa's 55 countries have enacted or embraced some form of regulation with the chief aim of protecting personal data**. Regionally, legislative tools such as the 2008 East African Community Framework for Cyberlaws, the 2010 Supplementary Act on Personal Data Protection of the Economic Community of West

[43] The continental dimensions of these challenges are addressed through continental digital collaboration.

African States (ECOWAS), and the 2013 Southern African Development Community model law harmonising policies for the ICT Market in sub-Saharan Africa have been developed. Continentally, the African Union developed the first pan-African framework with the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) in 2014, which has not come into effect but is currently being ratified. Regional competition laws and protocols on competition in the established Regional Economic Communities (REC's) apply to businesses that process data although they mostly do not explicitly refer to data. They include the 2004 COMESA Competition Regulations and Competition Rules, The EAC Competition Act (2006) and The EAC Common Market Protocol and the Protocol on the Establishment of an EAC Customs Union, The ECOWAS Supplementary Act on the "Adoption of Community Competition Rules and the modalities of their application within ECOWAS", and The SADC Protocol on Trade (2006) and the SADC Declaration on Regional Cooperation in Competition and Consumer Policies (2009). They address anti-competitive practices including abuse of dominance and also market structure through regulation of mergers and acquisitions. However details and approaches differ which presents challenges for businesses operating in multiple regions.

Other major initiatives on the continent looking at data policy

*The **Policy and Regulation Initiative for Digital Africa (PRIDA)** [44], within the framework of the implementation of this project , The African Union Commission established an Expert Working Group that contributed to the identification of the key harmonisation indicators and the development of a Monitoring and Evaluation (M&E) Model and Tool on Data Protection & Localisation which is ready to use by AU Member States and Regional Organisation to assess the extent of harmonisation and alignment of national laws and regulations*

***Smart Africa** is supporting the creation of a harmonised framework for data protection legislations in Africa through the Smart Africa Data Protection Working Group that aims at producing a mapping of legal frameworks, implementation guidelines for Smart Africa Member States as well as recommendations on enhancing harmonisation and collaboration mechanisms between Data Protection Authorities (DPAs).*

4.3 Situational analysis for data economy in Africa

Undertaking a situational analysis for the entire continent with its diverse legal, regulatory and political systems, and considering the unevenness of countries' economic development and digital readiness makes it inherently limited and overly generalised. The purpose of the high level SWOT analysis is to identify broadly applicable strengths and weaknesses of countries at a regional level and to identify the potential opportunities and known risks associated with the global processes of digitalisation and datafication that characterise the development of data economy for all countries but also what these mean specifically for African countries, within their broader developmental context.

[44] PRIDA is a joint initiative of the African Union (AU), the European Union (EU) and the International Telecommunication Union (ITU) that aims at enabling the African continent to reap the benefits of digitalisation, by addressing various dimensions of broadband demand and supply in Africa and by building the capacities of African stakeholders in the Internet Governance space.

STRENGTHS	WEAKNESSES
• Foundational regional data governance instruments • Regional Economic Communities (RECs) to support economic aspects of data policy initiatives • Regional and continental courts to enable harmonised dispute resolution • Emerging innovation hubs in region to demonstrate best practice across jurisdictions • Fewer and less developed competition, data and IP laws on data so greater potential for early, rapid continental harmonisation of laws enabling cross border trade	• Sub-optimal data connectivity and usage • Non-harmonised data governance regime • Inconsistencies in treatment of data in data protection, competition and intellectual property laws within countries • Localisation rules that limit the cross border flow of information necessary for local value creation and establishment of single market • Resource constraints in the evolution and implementation of data governance frameworks • Inadequate data infrastructure • Insufficient open government data to meet data demand • Inadequate provision, or access to, quality data • Uneven development of data standards. • Low penetration of foundational Digital ID Limited number of Data Protection Authorities (DPAs) many of whom are not well-resourced and/or fully empowered) • Need for cybersecurity capacity
OPPORTUNITIES	**THREATS/RISKS**
• If preconditions are met and enabling environments created there are opportunities for both public and private data-driven value creation through improved information flows and efficiencies. • Data use for improved public planning and service delivery and public and private sector coordination • With open data and interoperable standards underpinning integrated national data system, barriers to market entry may be reduced and opportunities for entrepreneurial development and innovation • Global efforts to develop and harmonise data policy and governance frameworks • Global efforts to coordinate taxation of digital and data services that have largely not contributed to national resource mobilisation efforts. • Emerging work opportunities for tech-savvy youth, to enhance local entrepreneurialism, local content development and innovation.	• Inability of some countries to overcome the challenges of creating enabling environments necessary to realising the opportunities • Failure to harmonise policy and regulatory frameworks to enable economies of scale and scope for data value creation and for all countries to enjoy benefits of a common digital market. • Constantly changing data protection and privacy risks • Discriminatory automated (algorithm-based) decision-making risk resulting from invisibility, underrepresentation of categories of people in datasets, and algorithm modelling shortcomings • Concentration in global data markets, preventing fair competition in local markets • Inadequate levels of international policy cooperation required to deal with global data issues - access, integrity, security, equity, rights and ethics.

4.4. Arising challenges in realising opportunities and mitigating risk

The uneven distribution of opportunities and risks associated with the development of the data economy correlates largely with the levels of human and economic development of countries, and the inequalities between and within countries. These are reflected in the strengths and weaknesses highlighted above. The ability of countries and regions in Africa to counter these trends is dependent on their **ability to create an enabling environment for data-driven value creation that is inclusive and equitable**. The purpose of the data policy framework is to provide a framework for countries to overcome some of the challenges of policy formulation in this dynamic and fast-changing area through common purpose and collective action. Through the creation of a harmonised enabling environment the strengths of countries can be leveraged and weaknesses mitigated for the development of an integrated continental data economy much more powerful than its individual parts.

The policy challenges that need to be overcome to create an enabling environment to realise the opportunities offered by globalised processes of digitalisation and datafication and to mitigate effectively identified risks for countries across the world should not be underestimated. These are currently the subject of several multilateral organisation reports (UNCTAD 2021, World Bank 2021). While some of the challenges relate to creating conditions for data-driven value creation at the national level that are highlighted in the situational analysis above and discussed below, the international and cross-border nature of data as global public goods requires more than ever before **regional and global cooperation f**or them to be realised at the national level and to mitigate associated risks which may arise from the use of data beyond national borders. While the data policy framework provides a high level framework for countries to develop national policies, these should be based on nationally consultative processes that take into account the local context, needs and institutional endowments of countries.

In creating this enabling environment in African Union member states and in the region, the following considerations arising from the situational analysis that may impact on the ability of country's to respond to the needs of a new data economy are flagged.

Digitalisation and datafication cuts across the public and private sector, the formal and informal economy, and social and cultural spheres, and requires a shift from traditional sectoral policies. Policy for the digital and data economy and society needs to be transversal to coordinate activities across the public sector and between the public and private sectors to meet national and regional objectives. It is at the same time important to consider the **specific sectoral data policies** to optimise and safeguard the diverse uses of different kinds of data (e.g. health data or climate data). Beyond noting this principle, the actual development of the several sectoral policies that will need to be developed is beyond the remit of this high-level framework. **Effective regulation of increasingly complex globalised markets is essential** to the ubiquitous backbone and seamless services needed for data services and applications to be deployed to meet the diverse economic and social needs, improve competition and promote African innovation. As in countries all over the world, policy makers will need to review and renew institutional arrangements for the governance of the data economy. Specialised regulators such as data or information regulators are required to deal with new issues of data governance, and both new and established regulators will have to engage in high levels of national and regional coordination. To ensure the African single market becomes operational, regulatory harmonisation is also essential for the integration of markets together with common online payment systems and cross-border trade facilitation and standardised cross-border taxation and duties. African states will need to caucus and

develop common positions to secure more favourable outcomes in forums of global governance to better serve African interests.

Transversal digital and data policy can manage the important interplay between competition, trade and taxation in a data economy. This presents an opportunity for African states to coordinate sectoral policies to support a flourishing data economy. For many African countries a risk that needs to be mitigated early on is the tendency towards market concentration and unequal wealth creation due to indirect network effects associated with economies of scale and scope. Data-driven digital markets are prone to 'winner takes all' outcomes. Amongst other factors, hyper-globalisation and digital interdependence contribute to monopolisation. This ultimately affects local competition and inhibits the global competitiveness of domestic data ecosystems. The challenges of market concentration, digital interdependence, and unequal distribution of wealth, particularly from base erosion and profit shifting, create the scope for incentives that encourage greater integration between mutual reinforcing priorities for usually siloed policy strategies in competition, trade and tax. Because of the increasing importance of regional and global governance, regional economic communities have an important role to play in the implementation of regional data policy through model laws and in supporting institutional- and human- capacity building.

Within the context of the African data ecosystem, **aligning the public policy objectives of taxation and data policy, particularly in the context of enabling the Single Digital Market, has been an intractable policy challenge** for many countries. Recent legislative and policy measures introduced by a number of African countries, within the context of the several multilateral and unilateral efforts at taxing the digital economy, may not be conducive to either the creation of a single market or to accessing international resources to realise global public goods and meet some of the preconditions for a competitive data economy on the continent. Tapping into new sources of tax revenue might allow African countries to eliminate excise duties on social networking and data services, reducing distortions to both the local market and the global tax system. The harmonisation of the tax regime for digital goods and services at the regional level, and alignment at the global level, may mitigate the risks associated with small data economies being unable to generate significant value and compete in global markets. These small data economies are typically unable to contribute to the scale and scope required for data-driven value creation and work with limited tax bases.

Legal clarity and certainty on emerging data issues is necessary in scaffolding a trusted and sustainable digital transformation. A global challenge is that the nature of data flows and digital infrastructure, threatens domestic data sovereignty. To exert control of data to safeguard sovereignty requires both infrastructure and law, but also the technical capacity to do so in a manner that can build trust. Transversal policies provide an opportunity for certainty on issues such as data ownership or custodianship and accompanying rights while establishing a comprehensive system of oversight over accessing and acquiring, and the analysis, storage, and dissemination of both personal and non-personal data. Ensuring consumer protection while enabling innovation is equally key to economic development and inclusion. Moreover, because different sectoral legal approaches serve different interests, countries are afforded the opportunity to re-invent a harmonised legal system that adequately balances corporate interests and relevant digital rights.

Creating **integrated and interoperable national data systems** in response to the emerging challenges enhances efficiencies and enables greater transparency and accountability. A common challenge found across the world is that when **data is of poor quality or not**

interoperable, it limits the capacity of firms and the public sector to engage in the sharing and analytics that can provide economic and social value to data. Insufficient avenues for access and limited commitment to open government data, amongst others, also impede an environment that fosters a strong data economy. The **provision of good data requires building a demand for data across institutional sites** (i.e. public sector, institutions and firms etc.). Extracting value from data requires not just control, but analytical and technical capacity developed in the public, private and other sectors.

Despite several countries introducing digital identification systems, **pervasive and interoperable digital identification systems remains a major social and economic challenge on the continent.** Digital identification systems enable identification for the purpose of transacting and interacting in a trusted data ecosystem. Foundational and functional identity facilitates digital services, but full coverage of foundational identity in particular remains both a social and economic challenge. The emerging regional frameworks on digital identity are starting to engage with this challenge directly. There are opportunities for decentralised, functional identity to be embedded in data protection frameworks. These may provide functional identity, while reducing the risks associated with personal data.

Another major challenge in this regard is the unevenness of economic and social data and particularly digital indicators in many countries to inform evidence-based policy formulation and to provide an accurate picture to global public databases such as within the UN statistical system. With the recognition of the strategic value of data, **priority needs to be given to the collection and storage of quality data to realise public value** and reduce existing information and associated power asymmetries within the public sector, between the public and private sector, and between both public and private sectors and citizens and consumers.

SMART AFRICA - Digital Identity

In 2020, Benin championed a Smart Africa flagship project to develop the Digital Identity Blueprint, was adopted by the Smart Arica Board, including its 32 Member States, the AU and the ITU with support of a range of other multilateral organisations and donors. The Blueprint proposes SATA as a platform to facilitate the trusted recognition of digital IDs between a range of actors through federated certification mechanisms. Pilot projects of SATA are anticipated to take place among Benin, Rwanda, Tunisia, and other Smart Africa Member States. SATA will serve as an agile and adaptable solution to enable interoperability between various public and private identity schemes on the continent.

Considering the specific African context and the slow pace of harmonisation efforts, the federated approach of SATA should allow for unilateral recognition of adequate legal frameworks by African States, with the support from a central and trusted certification authority. For this purpose, States need to strengthen their enforcement capacities, in particular the capacities of data protection authorities in monitoring and approving cross-border data transfers. The proposed framework will embrace state of the art technologies and be respectful of the countries' legislations and regulations. Governments should not be obliged to use specific technologies. The use of open standards and norms should guarantee a large diversity of technological choices by the States.

African countries face several well-documented, and interrelated challenges with respect to their uneven levels of **digital readiness** (International Telecommunication Union, 2019; World Economic Forum, 2016) that variably impact on their ability to respond to national and global challenges**.** These include the siloed development of policies and legislation, challenges around regional harmonisation of policies, a lack of institutional capacity, the ineffectively regulated competition amongst service providers, low levels of coverage, affordability and quality of broadband connectivity (Gillwald & Mothobi, 2019; Hawthorne, 2020).

Despite the adoption of continental charters, conventions and regional economic community model laws attempting to harmonise **Africa's response to the challenges posed by digitalisation and datafication, the ratification and implementation of them has been varied.** Getting wider adoption of the digital underpinnings for continental initiatives, such as AfCFTA, will be essential to realising the benefits of greater economic co-operation.

Standardised rules on cross-border flows is a prerequisite for the anticipated benefits of AfCFTA being realised. This can be done by using the operationalisation of the Agreement to facilitate better cross-border data interoperability and provide a harmonised continental approach to the data-driven digital economy. This can be done in a way that supports the socioeconomic benefits of digital trade and ecommerce, while ensuring that sensitive information remains secure and the relevant regulations on personal data protection are respected.

In response to previous waves of technological, and associated economic, regulatory and social innovation, **African countries have tended to be standards takers rather than standard makers.** Multilateral organisations, from the OECD to the World Intellectual Property Organisation and the World Trade Organisation, are reacting to the challenges of global data governance. Although Africa and African countries have, with some exceptions, not led global digital policies, there is an opportunity to change this. Multilateral, plurilateral and bilateral trade pressures to enable data flow with few restrictions are matched with pressures to concede intellectual property rights over data so that African countries face the prospect of data being both exploited and appropriated. In the absence of common Policy and commitment to common standards across the continent, it is difficult for most African countries to escape the currents of rapidly changing global dynamics. Therefore Coordinated action by and for Africa is required to collectively release the unlock the huge and transformative potential of data to develop an inclusive and sustainable Africa digital economy and modern society

Innovation in data communities use case

Typically cited examples of success in open data innovation are the emergence of particular innovation hubs across the region, chiefly in urban areas. Innovation hubs, as advocated elsewhere, can certainly be a site for social and economic open data successes; yet there are examples of open data innovation that can occur more organically just by the provision of quality open government data being made available. These can be driven by the needs of specific sectors – so for example, in agriculture, iCow was an app launched by a Kenyan entrepreneur that helped improve yields on cows for individual farmers by 100%. Other innovations in agriculture more centrally involving open data include, in Ghana, Farmerline and Esoko. Innovative firms can arise from open data, like the South African examples of OpenUp (Cape Town) and Open Cities Lab (Durban), which are socially focused enterprises both driven by open data. Ushahidi is an organisation (and software-as-a-service company) centred around an open source platform, which integrates crowd-sourced open data and maps it, and has been used to incredible social and governance effect in elections monitoring and crisis response throughout the region. Open data can have direct public cost savings as a result of innovations which emerge from data initiatives, creating a virtuous cycle: in an early partnership between OpenUp (then Code for South Africa) and the Southern African Programme on Access to Medicines and Diagnostics, a tool developed on open data on medicines pricings demonstrated to the Namibian government differentiations between pricing it was receiving on the drug Nifedipine, which after renegotiation led them to a direct cost saving of USD 1 billion a year.

5. Data Policy Framework

Data is increasingly recognised as a strategic asset, integral to policy-making, private and public sector innovation and performance management, and creating new entrepreneurial opportunities for businesses and individuals. When applied to government services, emerging technologies can generate massive amounts of digital data and significantly contribute to social progress and economic growth. The central role of data requires a high-level and strategic policy perspective that can balance multiple policy objectives. To unleash the economic and social potential of data while effectively protecting privacy, intellectual property and other policy goals, national data strategies should be formulated in the context of enhancing international interoperability.

The development of a Continental Data Policy Framework is necessary to realise the shared vision and common approach of an integrated African data ecosystem. This data ecosystem should support the establishment of an Africa Digital Single Market (DSM), foster intra-Africa digital trade, and boost the development of inclusive, data-enabled entrepreneurship and businesses. This is envisioned by both the AU Digital Transformation Strategy (DTS) and in the forthcoming Phase II and Phase III negotiations of the AfCFTA, where guidelines on Trade in Services and the E-commerce Protocol are expected to be established.
The Framework provides high level principle-based guidance to member states in their development of data policy appropriate to their conditions. It identifies the key principles of effective data governance and strategies for implementation at the national, continental and international levels. This includes guidance on the appropriate institutional, administrative and technical procedures and safeguards that need to be implemented. The aim is to ensure national and sub-regional data ecosystems are built on trusted, interoperable digital infrastructure and processes which advance a harmonised continental data system that enables equitable and sustainable economic growth and development for all of Africa's people.
The Framework reaffirms the importance of the AU's commitment to stable, harmonised and predictable regulatory frameworks and contextually relevant policies to facilitate:

- incentives for efficient investment in foundational digital data infrastructure and foundational digital systems;
- institutional arrangements that permit the optimal interplay between state, markets and regulatory institutions to enable public and private value;
- building human and institutional digital capability;
- creating value from responsible data use, fostering sustainable equitable growth, and enhancing shared prosperity from the data economy;
- improved distribution of opportunities both for the use of data services and for production and data driven-value creation within and between countries; and
- effectively regulated environments that promote fair competition and the resource allocation efficiencies that produce positive consumer welfare outcomes.

5.1. Guiding principles of the framework

The Data Policy Framework needs to align with the AU values and International law to achieve greater unity and solidarity between African countries and their people, ensuring balanced and inclusive economic development, including promoting and protecting peoples' rights through the African Charter on Human and Peoples' Rights and other relevant instruments.
In the spirit of fostering regional prosperity, economic growth and development, social progress and coordinating continental efforts, the following high-level principles guide the framework.

- **Cooperation:** African Union Member States shall cooperate in exchanging data, acknowledging data as a central input of the global economy and the importance of the interoperability of data systems to a flourishing African digital single market;
- **Integration:** the Framework shall promote intra-Africa data flows, remove legal barriers to data flow, subject only to necessary security, human rights and data protection;

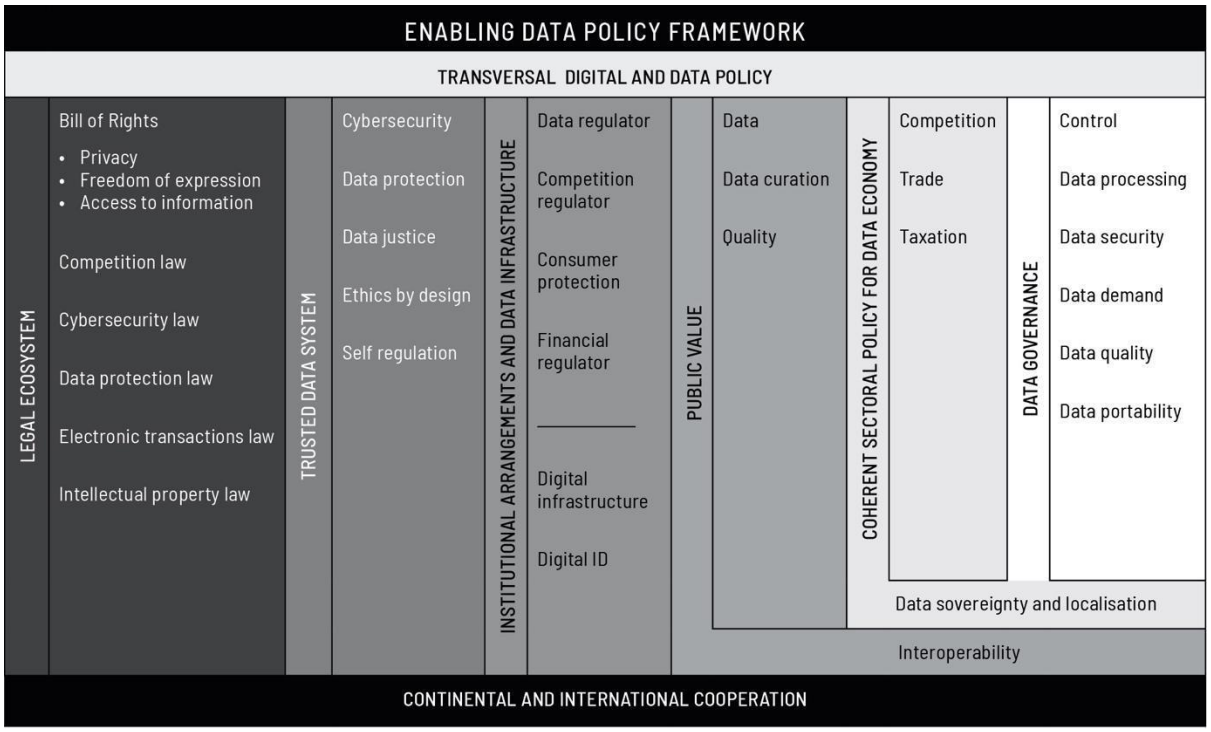
- **Fairness and inclusiveness :** in the implementation of the Framework Member States shall ensure it is inclusive and equitable, offering opportunities and benefits to all Africans, and in so doing seek to redress national and global inequalities by being responsive to the voices of those marginalised by technological developments;
- **Trust, safety and accountability:** Member States shall promote trustworthy data environments that are safe and secure, accountable to data subjects, and ethical and secure by design;
- **Sovereignty**: Member States, AUC, RECs, African Institutions and International Organisations shall cooperate to create capacity to enable African countries to self-manage their data , take advantage of data flows and to govern data appropriately;
- **Comprehensive and forward-looking :** the framework shall enable the creation of an environment that encourages investment and innovation through the development of infrastructure, human capacity and the harmonisation of regulations and legislation; and
- **Integrity and justice:** Member States shall ensure data collection, processing and usage is just and lawful, and data should not be used to discriminate unfairly or infringe peoples' rights.

5.2. Data definition and categorisation

There is no agreement on how data is defined, probably as a result of the very many different types of data that are collected and used, and their varying purposes and values. Without recognising these different kinds of data and the various roles it can perform, governments will not be able to effectively address issues such as personal data protection or competition. Better measurement of data and data flows and their role in production and value chains will also help support policy making.

5.2.1 Personal and non-personal data

Although data, conceptually, means different things for different communities and depending on the context, an important concept which is at the core of the data protection regulation, is that of personal data. Defining specific types of data as personal may help data protection authorities protect data subjects' rights more efficiently but there are limits to this approach.



There are numerous ways that data can be categorised that affect the appropriate policy and regulation of that category, among the most important dimensions are as public or private intent and traditional or new collection methods (UNCTAD, 2021; World Bank, 2021).

As data protection authorities start implementing personal data protection legislation, they should provide industry with definitional clarity on how to differentiate between personal and non-personal data, to enable the collection, storage and processing of data by companies compliant with data protection regulation. This will also reduce the risk of non-compliance during data collection, storage, and processing. It is important that data policies, and data regulations share the same categorisations of data to ensure policy cohesion and enable compliance.

5.3. Enablers to drive value in the data economy

Reaping the benefits from data is highly dependent on enabling regulatory and policy frameworks that facilitate obtaining useful data; enhancing human, institutional, and technical capabilities to create value from data; encouraging data sharing and interoperability; and increasing legitimacy and public trust in the state to manage citizens' data in a responsible manner. Furthermore, the data infrastructure that enables an integrated data system is a key strategic asset for countries. The environment created by the interplay of elements in the data ecosystem and the nature of the relationships and non-linear processes between and within them, determine the interventions to create incentives for technology investments that are required to drive growth in the data economy. These conditions are shaped by the market structure, the competitiveness of the services that arise from it, and how effectively the market is regulate.

The digital economy permeates various industries and social activities, and data policy needs to be located within the context of the wider complex and adaptive digital ecosystem. As discussed, this has implications for other policy areas, including commerce, trade and taxation. States should invest in data capabilities and complementary assets to support policy making.

Investments in data-related innovation and research and development (R&D), as well as in capabilities to harmonise standards, skills and infrastructures, can enable governments to

develop better data related policies across the board. Issues of trust and ethics are equally important, while evidence-based and consultative regulations need to be prioritised. Recommendations:

- Member States of the African Union should promote research, development and innovation in various data related areas including, Big Data Analytics, Artificial Intelligence, Quantum Computing as well as Blockchain
- All stakeholder groups, including governments, should build data analytic and data management capabilities to facilitate the use of quality data and trusted interoperable systems. However it is important to remember that in many countries the largest collective producer and collector of data is the state. Therefore many of the observations included in the discussion on data governance below have particular bearing on the actions of governments.

5.3.1 Foundational data infrastructure

5.3.1.1 Broadband and data access and use

Defining the problem

There are access barriers to broadband infrastructure that prevent people joining the data economy even as users. According to the ITU Broadband Commission *Connecting Africa Through Broadband Report*:[45] "Nearly 1.1 billion new unique users must be connected to achieve universal, affordable, and good quality broadband internet access by 2030, and an estimated additional $100 billion would be needed to reach this goal over the next decade." Despite this, and a myriad of contextual constraints, Africa has a vantage position to evolve an innovative data ecosystem, being less hampered by legacy data infrastructure, and having a relatively lower spectrum utilisation and congestion levels (Saint & Garba, 2016). While fixed broadband penetration in the region is less than one percent, mobile internet is more ubiquitous with a lower adoption cost.[46] Therefore, the evolution of Africa's data ecosystem will primarily be enabled by mobile broadband networks.

Recommendation

To accelerate the domestication of the framework, there should be a massive robust digital infrastructure roll-out across AU members along with sufficient capacity .Member states should prioritise attaining meaningful connectivity and affordable internet that onboards more users and drives up demand for infrastructure services. For a more effective uptake and utilisation of data in the region, complementary infrastructure deficits which limits the utility of data needs to be addressed.

Actions

Member States will need to evolve policies that:

- proscribe prohibitive 'right of way' broadband cable fees and support infrastructure sharing;
- prevent anti-competitive practices arising from dominance in infrastructure markets;
- invest in public Wi-Fi and complementary technologies;
- adopt innovative spectrum utilisation techniques such as dynamic spectrum allocation and access, and the leverage of digital dividend (spectrum bands largely expedited by

[45] https://broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf

[46] ICT Data and Statistics Division, Telecommunication Development Bureau, "ICT facts and figures 2016," International Telecommunication Union, Geneva, Report, 2016.

the analogue to digital broadcasting migration) to expand broadband access for underserved rural areas;

- promote the transition and adoption of IPv6[47], as IPv4 resources become more depleted globally;
- invest in national backbone and cross-border connectivity infrastructure such as Internet Exchange Points (IXPs) at both national and regional levels to leverage available international bandwidth, lower internet access cost and enhance data access speeds within the region; and
- leverage innovative models for data infrastructure funding.

5.3.1.2 Data infrastructure

Defining the problem

Foundational data infrastructure that facilitates data systems and allows for the sharing, gathering, and storing of big data, or the manipulation of existing data sources, will impact how governments are able to respond to the challenges related to data availability, quality and interoperability, and approach considerations related to legitimacy and public trust.

Foundational data infrastructure refers to a wide range of technologies that facilitate the intensive use of quality data, including hard and soft infrastructure[48]addressing existing "traditional" ICT infrastructure deficits will have to be made in parallel with creating architecture to support increased datafication. It also includes infrastructure resources such as Digital Identification to enable secure online transactions and presence. This Framework will focus on three data infrastructure aspects that require mutually reinforcing policy considerations and also influence data governance: cloud services, big data and platformisation.

Developing public data value from cloud-computing infrastructure and software that complements big data processing and analytics will need to be informed by well-developed security and trust models for cloud storage and processing of sensitive or proprietary data, API management, and support of equitable data ecosystems markets. Beyond the digital infrastructure inadequacies in many governments – including weak enablers to accommodate an environment for supply and consumption of cloud services – African countries face a multitude of challenges in responding to infrastructure requirements as this infrastructure is often supplied by and procured from private Foreign Service providers.

This implies that to leverage opportunities associated with digital transformation, other challenges such as intermediary liabilities, jurisdiction boundaries, interoperability, and sovereignty issues, to name a few, will need to be considered. These challenges underscore the need for collaboration and partnerships in many African data ecosystems to strengthen fundamental enablers of successful data driven activity markets across different points in the data value chain, regardless of domestic digital maturity and endowments.

The technological, organisational, legal and commercial regulation and legislation in place will impact the efficiency of the shared infrastructure to facilitate various data market participants with access required to operate in the data market. Data ecosystems should be able to support various application domains, allow data exchange and integration at different stages of the data value cycle while preserving data provenance and integrity.

Cloud services

---

[47] Internet Protocol version 6 is the most recent version of the Internet Protocol that provides an identification and location system for devices on networks and routes traffic across the Internet.

[48] See Annex for full definition

It is useful for policy purposes to distinguish between "cloud services" and "cloud-based services." The main benefit offered by cloud services is cost savings through enhanced systems efficiency. For example, resource-constrained public sector and small, medium and micro enterprises (SMME's) can reduce capital expenditure on IT equipment including internal servers, networking equipment, storage resources and software by shifting to a utility-based cloud services model.

Interoperability in cloud provision is a critical factor as this allows flexibility and enables users to switch between one cloud provider and the other. Other benefits of cloud computing include reduced spending on energy consumption as well as lower demand for systems management and maintenance by shifting the management of IT resources to third-parties. As a result, funds can be shifted to customer-facing activities and better public service delivery. However, as there are certain factors that support a conducive environment for cloud-based services, making provisions to adopt new technologies must be done in parallel with addressing structural digital divide challenges (human capital, infrastructure, etc.). These processes must be mutually reinforcing and suited to Member States economic realities. Developing data value from cloud-computing infrastructure and software that complements big data processing and analytics will need to be informed by well-developed security and trust models for cloud storage and processing of sensitive/proprietary data, API management, and support of equitable data markets.

Big data

Massive amounts of data are being produced - including as by-products of other activities (such as by social networking platforms when they create profiles of their users for advertisers) - and used for the development of products, services and entirely new forms of businesses, with the potential to generate substantial efficiency and productivity gains. This also holds potential for the public sector which sits on vast amounts of data that could be used for 'big data' analytics by improving decision-making, forecasting and allowing for better consumer segmentation and targeting. The advantages of scale and scope related to network effects have produced near monopoly positions, which have been further enhanced through mergers of smaller, new providers of services that do not at first glance appear to be in the same market, such as Facebook and WhatsApp. This makes it nearly impossible for local players to compete (Arntz et al., 2016).

Platformisation

Datafication has also created entirely new business models and modes of value creation and value extraction. One of these is 'platformisation', which facilitates transactions and networking as well as information exchange, aggregating multiple sellers and buyers on a single platform.

With digital trade and e-commerce platforms increasingly underpinning global and cross-border activity, the integration of traditionally distinct areas of regulation and policy priorities have become increasingly important and intertwined across geographical boundaries. However, policies such as data localisation will not be plausible without the necessary structural and institutional requirements for their effective evolution and implementation, in particular reference to digital capabilities (Andreoni & Tregenna, 2020)

Recommendations

Using data as a tool to enhance public interests will require states to strengthen domestic data infrastructure and will need robust stakeholder engagement at the national, regional and global levels. Developing comprehensive enabling data policy frameworks should be accompanied by time-sensitive implementation strategies across different domestic mandates to ensure accountability and transparency.

Member states should prioritise resources to ensure that there are incentives to increase investments in digital infrastructure, data platforms, and software capabilities to leverage big

data. Data infrastructure investments must support the digital social contract. State efforts to enhance Interoperability, quality, and public administration of data must also complement and enhance public digital systems such as digital IDs, digital payments, and open data flows, as far as possible. The appropriate infrastructure is also a necessary component of any interoperable integrated data sharing system. Furthermore, reusing or repurposing data typically requires well-functioning data systems that facilitate the safe flow of data in machine readable formats that make the data valuable to many users.

Actions

- As opposed to focusing on the significant upfront investment to replace depreciating legacy ICT equipment, Member States should leverage economies of scale and scope to adopt infrastructure that supports facilitating benefits offered by cloud services and other new technologies that support data value creation
- Tax, trade (including investment and innovation) and competition policies must be coherent, complementary, and adapted to the data driven digital economy, particularly to inform infrastructure development strategies
- Member states must ensure local firms participate in value chains of foreign software as a service (SaaS), infrastructure as a service (IaaS) and platforms as a service (PaaS) providers for state procurement and create incentives to have local SMMEs in data value chains across industries. This can be done by ensuring tax, trade (including investment and innovation) , and competition policies are coherent, complementary, and adapted to the data driven digital economy
- Adopt more sustainable electricity generation models, domestically and across the region to ensure foundational digital infrastructure supports sustainable domestic and cross-border data activities that have less extractive impacts on the natural environment.

Data governance

- Creating data portability rights - including for non-personal data, to make it easier for customers of cloud services to switch between providers.
- Develop contractual standards for public organisations (that can be used by SMEs too), that protect their rights to access, retrieve, delete, etc. the data (including non-personal, again) that is processed by cloud providers.
- Develop Fair, Reasonable and Non-Discriminatory (FRAND) licensing obligations for platforms and cloud providers who have access to datasets that become a vital resource to enter a market.

5.3.1.3 Digital ID

Defining the problem

With the African continent hosting the highest percentage of people without legal identity and subsequently uncovered by civil registration and denied essential social services offered by states such as healthcare, basic education or food services[49]. The digital economy,

[49] See https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity

however, offers opportunities to redress inequalities such as socio-economic and structural exclusions suffered by minority groups on the continent.
Digital ID, as a form of personal data expression, must be constructed and implemented cohesively in line with overarching data governance frameworks. Digital ID is facilitative for both private and public sector purposes within a data economy, but demands a robust trust-guided framework to mitigate against the potential harms like personal data abuse, exclusion, or discrimination based on inaccurate (or unfair) data representation, that may accompany such initiatives. Further, although private-public partnerships have the potential to expand the public delivery of state services and boost socio-entrepreneurial innovation such collaborations can potentially exacerbate inequality (through data misuse) on top of the harms mentioned above. The frameworks adopted by existing national identity authorities/agencies should therefore be revised to reflect these opportunities, risks and harms.

Recommendations

A fair and trustworthy digital identification system is a central prerequisite to combine and repurpose public administrative data with other types of data across various use cases. Regional data policy activities should align with those occurring under concurrent Digital ID activities. Public sector digital identity initiatives must remain guided by data governance frameworks, whether foundational or functional[50].

5.3.2 Creating legitimate and trustworthy data systems

Defining the problem

A trusted data environment requires users to trust the entire political and economic system underpinning the data economy. Fundamental aspects of this kind of system include safeguarding basic human rights through the rule of law; institutional arrangements and regulations that are established through consultative and transparent processes; and requiring that institutions responsible for overseeing the use of data, as well as public and private data producers, are accountable for the use of public and personal data. Inclusion and diversity of people who manage and oversee data environments, for example through gender diverse teams, is important to build trust. Several African countries already have many of these aspects, the continental challenge is to ensure that all countries have all the necessary aspects and that these are appropriately adapted to rapidly evolving data technological and economic challenges. The framework sets out all the essential components of legitimate and trustworthy data systems to enable benchmarking by countries as to whether they have some or all of the components fully in place.
Trust in data transactions, statistical data, and data-based decision making must therefore be sustained by a transparent and robust legal and regulatory framework that simultaneously safeguards against data harms and supports enablers that facilitate access to data, data sharing, and data alterations in a responsible manner. A strong trust framework, and the institutional capacity to support this framework, will allow governments to create value from data, minimise public-private data asymmetries, and curb uncompetitive behaviour in data ecosystems (Macmillan, 2020).
In this context of building a trusted digital ecosystem, three key interrelated areas need specific consideration: cybersecurity, cybercrime, and data protection. The role of ethical design and positive regulation to ensure justice outcomes is also worth highlighting.

5.3.2.1 Cybersecurity

As technology evolves and disrupted technologies are adopted, new threats and unwanted risks are created. This not only impacts assets, infrastructures and networks, but also

[50] The African Union Commission is developing an Interoperability Framework for Digital ID that will provide a detailed set of recommendations to member states on introducing and safeguarding digital ID systems.

economies, societies, and people, with the most vulnerable being the most affected. Because of this, the use actors make of disruptive technologies and the public and private sector norms, rules, and practices to govern security, may impact on people's fundamental rights of equity, dignity and security.

While policies, laws and regulations can be tools used to push back against threats and protect people from risks, they can also be used to normalise or legitimise systems of oppression and repression. Therefore, any cyber policy response aimed at strengthening data security should consider elements of proportionality (including legality, legitimate aim, necessity, and adequacy) as the most important requirement that must be satisfied in any form of limitation of online human rights.

5.3.2.2 Cybercrime

The data ecosystem highlights both the opportunities and risks of a vast network of linked public and private systems. Due to the transnational nature of cybercrime and cyber operations, policy on data security is mostly shaped in multilateral global or regional forums. While African participation in these forums has increased, the involvement of non-state African actors is still limited. Moreover, an emerging policy challenge is to evaluate what capacity is needed nationally to implement regionally and globally agreed conventions on cybercrime, and voluntary and non-binding cyber norms.[51]

5.3.2.3 Data protection

The risks of unlawfully possession of processed data are borne chiefly by data subjects themselves, and not the entity extracting value. Because of this, mechanisms and principles for mitigating against privacy risks must be central to any national and regional policy frameworks that seek to harness the potential of data economies.

While this requires developing sound data governance institutions and laws, these laws also need to be responsive to the particular contexts in which they are being implemented. These include consideration of the socio-economic and technological realities and capacities of the public. Stated differently, a data policy framework needs to develop policy and regulation that is able to acknowledge the realities of a citizen's capabilities and functionalities, along with the risks that accompany digital developments and lead to the unequal distribution of benefits and harms (Sen, 2001; van der Spuy, 2021).

For example, with significant numbers of people digitally and otherwise illiterate in Africa, digital mechanisms of informed consent may not be sufficient to protect the rights of people. There is a risk that for many people commonly use digital means of obtaining consent; such as selecting a button linked to a lengthy legal set of terms does not actually amount to informed consent because the action that is meant to constitute consent may not be an informed act or understood at all by the person doing it. Other means of data stewardship such as data trusts, that are emerging globally, that ensure that the rights of people over their data are upheld, are discussed below. Similarly, the dominant framing of data governance is generally equated with data protection and data protection with privacy. It is largely understood as an individual right, and individual challenge. However, there are issues of community and collective rights that may be important to foreground in dealing with issues of public interest.

5.3.2.4 Data justice

The concept of data justice promotes a broader view than data protection. While a rights-preserving data policy framework will be essential to safeguarding the rights of people, the individualised notions of privacy in current data protection normative frameworks may not be

[51] Deficits in implementation capacity have been observed across five dimensions: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training and skills; legal and regulatory frameworks; and standards, organisations and technologies.

sufficient to ensure more equitable inclusion in a trustworthy data economy. Data justice is a concept that has been gaining traction in response to the exponential adoption of data-driven technologies worldwide, particularly artificial intelligence (GPAI 2021[52], Tyler 2019). It seeks to ensure that the increasing reliance on data, especially for automated decision-making, does not perpetuate historical injustices and structural inequalities. It addresses the question of fairness in response to the degree to which people are visible, represented and underrepresented and discriminated against as an outcome of their production of digital data. Data justice also extends beyond notions of political rights and justice to social and economic rights and regulation that is necessary to redress inequities and enable people to exercise their rights. There are many other areas of data governance in relation to data availability, accessibility, usability, and integrity that impact on equitable inclusion. If these are regulated in the public interest, they could contribute to a better distribution of the opportunities not only for the consumption of data services but for the production of services.

Recommendations

Member States should seek to establish a reliable and trustworthy data environment through cybersecurity, protection of personal data, the rule of law and capable, responsive, and accountable institutions. They should establish trust in data governance and a national data system through ensuring legitimacy throughout the system. This includes systems and standards that guarantee public and private sector compliance, government itself adhering to personal data protection rules, and government sharing public data.

Actions

- Safeguard basic human rights in the digital environment through the rule of law;
- Ensure institutional arrangements and regulations are established only through inclusive, consultative and transparent processes;
- Ensure institutions responsible for overseeing the use of data, as well as public and private data producers, are accountable for the use of public and personal data to those whose data is used.
- Strengthen cooperation with other DPAs to ensure sufficient safeguard, reciprocal protection of personal data as well as individual and collective digital rights across the continent.
- Strengthen Mutual Legal Assistance Agreements and activities across states for the investigation and prosecution of cybercrimes.
- Ensure institutions responsible for overseeing the use of personal data are empowered to have powers of entry and inspection for purposes of enforcement of privacy and data protection laws and regulations.
- Further ensure institutional responsible for overseeing the use of personal data have the following corrective powers in relation to correcting infringement of aspects of misuse and abuse of personal data:

[52] The Global Partnership on Artificial Intelligence has developed a project which aims to fill a gap in data justice research and practice that provides a frame to help practitioners and users to move beyond understanding data governance narrowly as a compliance matter of individualised privacy or ethical design. The project seeks to include considerations of equity and justice in terms of access to and visibility and representation in data used in the development of AI/ML systems. https://gpai.ai/projects/data-governance/data-justice/

- Issue warnings to a data controller or data processor that intended processing operations are likely to infringe provisions of the relevant data protection laws and regulations.
- Issue reprimands to a data controller or a data processor where processing operations infringe provisions of the relevant data protection laws and regulations.
- Order a data controller to communicate a personal data breach to affected data subjects.
- Impose a temporary or definitive limitation including a ban on personal data processing.
- Order the suspension of data flows to a recipient in a third country or to an international organization that does not provide adequate protection similar to that of the data exporting country.

- Institutions responsible for overseeing use of personal data should be empowered to either assist or seek court's indulgence to assist a person who has suffered material damage as a result of an infringement of their personal data to receive compensation from a data controller or data processor for the damage suffered.

5.3.2.5 Data ethics

An important way to reduce risk and mitigate harms through the application of new data technologies is through contextually appropriate data ethics. Codes of ethics should be developed by all stakeholder groups working with data, including researchers, industry associations and data experts. These codes of ethics are valuable for guiding the use of data, and the processes of designing and implementing data systems, including embedding them in computer code in the case of developing algorithms.

However, codes of ethics have been criticised as representing the views of limited demographics, mostly defined by the corporations and technologists. Ethical codes can also relieve corporations of regulatory accountability when used as a form of self-regulation, and can be insufficient in enabling the fundamental rights of people when using technology.

Ethics, working together enables trustworthy data systems by providing the kind of practical and technical details that support laws since the later are usually of more general application than specific ethical codes but also sometimes less quickly adaptable to new technologies. Ethics operate prospectively enabling ethical design while laws tend to be enacted and operate retrospectively. Ethical codes of conduct should embody digital rights and support compliance with international and national law.

The AU supports efforts to make ethical codes more inclusive through processes that take into account the voices of citizens, consumers, marginalised and underrepresented people. Nevertheless, mechanisms for ensuring adherence to ethical codes as well as for updating those codes, are underdeveloped.

Human rights treaties – as the product of consensus processes between the legitimate representatives of citizens – enjoy greater legitimacy than codes of ethics, and are legally enforceable when enacted at the national level, and through regional adjudication. While these treaties sometimes do not have the specificity necessary for data ecosystems, digital rights, which have been formulated variously by civil society amongst others and draw on the human rights framework, provide the kind of specificity that can be drawn on. Although existing human rights bodies and adjudicators have the requisite capacity to develop rights in response to data issues, their legal mandates may not sufficiently empower them to do so.

Recommendations

Member States should encourage the development and adherence to codes of ethics that are responsive to the African context, and which promote digital and human rights. This means people who work with data, regardless of the sector they work in, must respect rights and adhere to these ethical standards. These codes ought to take note of gender considerations within the African context ensuring they reduce harms and exclusion of women and girls. It is impractical for member states to legislate that all technologies and technology providers dealing with data adhere to particular ethical codes since many of these technologies are designed, built and operated in other jurisdictions. Member States should however encourage the adoption of these codes of ethics by themselves making use only of technologies and technology providers that adhere to approved codes of ethical conduct.
Besides any regulatory or judicial legal recourse available in a country, there is also scope to consider empowering existing human rights mechanisms at the national, regional and continental level to adjudicate uses of data.

Actions

- The data industry and research communities using data need to formulate and implement codes of practice, including the principles of responsibility and ethics by design through processes that include those whose data is affected;
- Member States must require rights-compliant ethical frameworks in public procurement processes;
- Members should include the assessment of data codes of ethics in the mandates of existing human rights bodies such as Human Rights Commissions.

5.3.3 Institutional arrangements for regulation of complex adaptive systems

The following are key considerations in aligning the regulatory context in a country with the requirements of a data economy. The regulation in data economies requires future-facing agile regulatory decisions in the face of uncertainty. Thus regulators require both the mandate and the confidence to regulate proactively. Complex adaptive regulation responds not only to the challenges of rapid change and uncertainty, but the complexity of data ecosystems characterized by multi-factor dynamics.

5.3.3.1 Building capacity of regulatory bodies

Rapidly intensifying processes of digitalisation and datafication present new regulatory challenges in the traditional areas of competition and consumer protection, and entirely new areas of regulation including the protection of peoples' personal data and algorithmic governance to ensure people are not discriminated against. While the traditional principles of independence, transparency and accountability continue to inform the effective regulation and governance of data, policy makers and regulators need to develop new capacities to face the challenges.

5.3.3.2 A shift away from regulatory silos

While the different institutional endowments will determine whether existing regulators have the capabilities to manage new areas of governance, it is clear there will need to be a shift from regulation within traditional sector silos to integrated or at the very least coordinated regulatory action. This is made possible by the development of traversal digital strategies and policies that recognise the cross-cutting nature of digitalisation and datafication. This is essential to create the necessary coordination across the various sectors of public services impacted by the data economy, and at the same time to meet sector-specific data governance needs

The African Network of Information Regulators provides an example of regional collaboration to establish national data regulators, raise awareness of new information and data governance, provide governance for cross-border data flows and cooperate with regulators internationally. It does this to align governance particularly in relation to the proportional and standardised response to data breaches and violation rights.
National regulators and policy makers have a role to play at the international arena. Intensify international cooperation on cross-border data flows to ensure that data localization requirements and other restrictions on cross-border data flow do not unduly interfere with cross-border communications and the economic and societal benefits that global data networks make possible and are minimally trade-restrictive, while promoting trust.
Encourage regional and international cooperation on data privacy and cybersecurity initiatives to streamline the patchwork of data privacy and cybersecurity rules and practices into common regional or global standards and laws and allow free flow of data and digital trade (GSR 2021).]

AREA OF REGULATION	TOPICS OF POTENTIAL COLLABORATION WITH THE DATA REGULATOR
Telecommunications	Availability and quality of foundational infrastructure to enable data services
Competition	Concentration, mergers and acquisitions, anti-competitive practice in digital and data markets but also pricing and market structure's effect on security
Consumer protection	Digital devices and services, e-commerce
Commerce/trade	Digital taxation, e-commerce, digital services, digital financial services
Finance	Finance blockchain, cybersecurity, financial inclusion, mobile financial services, privacy
Education	Online child protection, schools connectivity, availability of data for acquiring data skills

Source: Adapted from TGM 2020 in ITU World Bank 2020.

5.3.3.3 Data regulator

The capacity of sector regulators to be effective is determined, at least to some degree, by the institutional arrangements and the autonomy of regulators to implement policy. The levels of efficiency and innovation that enable the evolution of the ecosystem depend on the availability of skills and competencies of people and institutions at each node within the ecosystem to harness the benefits associated with integrated networks for economic development, and social and political engagement. Developing an integrated data system at a national and regional level is also highly dependent on enabling regulatory and policy frameworks that facilitate obtaining useful data, enhancing human and technical capacities to create value from data, encouraging data sharing and interoperability, and increasing legitimacy and public trust in the state to manage citizen data in a responsible manner. Creating the conditions that allow for the necessary access to data while safeguarding rights will require building institutional capacity and capabilities to optimise the potential of data, and developing enforcement mechanisms.

5.3.3.4 Competition

As regulators in Africa struggle to introduce and enforce traditional competition regulation, there is a danger that static competition regulation to govern dynamic and adaptive systems may inhibit innovation and damage the underlying technology that enables innovation. For example, regulation that focuses on curbing dominance in only the app layer of the Internet could negatively impact and even harm the entire internet and its infrastructure. Regulators

need to be cautions of instrumentally apply single-sided market competition rules based on static efficiency models to new data platforms and products based on dynamic efficiency that may produce innovative complementary products (such as WhatsApp) that enhance consumer welfare and choice or even opportunities for local competition on their platforms while being dominant in the underlying global market, (Facebook).

Platforms are different from traditional operators in the markets as they are constituted by numerous relevant markets that have multiple 'sides', each with specific competition dynamics. Similarly, Over the Top (OTT) products and services can appear to be vertically integrated when in fact they are complementary and competition enhancing. These kinds of challenges require equally adaptive regulators able to manage their complexity in the public interest.

5.3.3.5 Consumer protection

As consumer protection authorities are not responsible for one specific sector, in exercising their functions they have generally relied on other sector-specific regulators. Clear, strong and enforceable rules related to data governance can provide adequate defence for digital consumer protection while creating a predictable, structured framework for doing digital business. Agile regulatory protocols and mechanisms able to adapt to rapidly changing technologies and conditions can go a long way towards enhancing trust in the digital ecosystem. These include complying with requirements related to the access to non-personal data retained by digital platforms, the transparency of certain essential algorithms used by digital services, the portability of essential data of structuring platforms, and the interoperability and maintenance of APIs (International Telecommunication Union, 2020)

A way of increasing transparency on the use of consumers' data is the creation of transparency portal, but this is dependent on the data regulator having the resources to establish, monitor and enforce breaches. This provides people secure access to a portal where they can see the history of when and with whom their personal data was shared enabling them to challenge data shared or used without their consent. This may not apply to certain categories of public interest data sharing of data accomplished through pseudonymising or anonymisation of the data.

Recommendations

AU Member States should have adequate regulations, particularly around data governance and digital platforms, to ensure that trust is preserved in the digital environment. Data regulators should have the requisite powers to enforce compliance with data regulations such as powers to issue warnings, penalise for breaches, award compensation for victims of data, and to cooperate with other agencies including enforcement agencies.

Actions

- Members with data regulators should assess whether the existing enforcement powers are sufficient.
- Members creating data regulators should consider a range of enforcement powers, and in addressing resource constraints how data regulators could potentially rely on other agencies for enforcement.

5.3.4 Rebalancing the legal ecosystem

Defining the problem

A number of the different but overlapping branches of law, such as data protection law, competition law, cyber security law, electronic communications and transactions law, and the different categories of intellectual property law deal with data. However they may conflict or contradict each other. In contrast to data protection that applies only to data that can be related to an individual, competition regulation applies to data when control over data has an

anti-competitive effect. Concentrated control over data, including data flows and data analytics, implicates not only barriers to market entry, but the public interest. Concentration of data, data flows and data systems substantially increases the likelihood and damage that can be caused by cyberattacks and data breaches since it leads to a single or a few points of failure that can have large scale consequences. These concerns are not within the purview of many competition authorities but should be since there are public interest concerns. Competition authorities can be mandated to avoid structural centralisation of data firms that increases society-wide risks of cyber-attacks or massive scale data breaches. Access to data is generally pro-competitive but may be in tension with other laws such as intellectual property claims over data and databases and privacy and data protection.

While it is generally accepted that raw data is not protected by any recognised property right, claims have been raised over data based on the different types of intellectual property; copyright, sui generis database protection, trade secrets and patents. None of these grant ownership over data, as such. Sui generis database protection is a uniquely European Union law, confined to Europe. In a few common law countries copyright has been extended to databases and compilations of data but even these countries have different rules with some courts extending copyright merely for effort of compilation while others require creativity. Copyright is intended to reward human authors and its application to databases compiled by computers is undetermined. Disputes between competitors overuse of industry standard databases straddle copyright and competition law. A court ruling (Discovery Ltd and Others v Liberty Group Ltd ZAGPJHC 67, 2000) offers a solution that upholds both data protection and competition: in such disputes if the data is personal in nature, it is 'owned' by the data subject and competitors may not exclude others from accessing this information. While the application of intellectual property laws to data are still being resolved the rights of people over their personal data should be treated as stronger than any intellectual property claim over that data because data protection is so important to building data economies.

Trade secrets may also apply to data in some circumstances but precisely which circumstances are unclear.

The application of intellectual property laws is both complicated and undetermined, but it is at least clear that claims over data based on intellectual property, even though contested, potentially jeopardise the beneficial flows of data and data protection.

Cybercrime laws prohibit the unauthorised access, use or alteration to personal data or ID systems. As reiterated throughout the policy framework, safety and security are essential to the effective implementation of the policy and a threshold, though not sufficient, requirement for building a trustworthy system. Cybercrime laws by determining the ways in which data is accessed, used and distributed, have the potential to raise the barriers of entry into the data economy. The Malabo Convention enacted by the African Union and specifically tailored for the region deals with both cybercrime and data protection. However, it is not yet in force as it awaits ratification.

Members have an opportunity to re-invent a harmonised legal system that adequately balances competing interests.

Recommendation

In order to ensure equitable and safe access to data for innovation and competition, member states must establish a unified legal approach that is clear, unambiguous and offers protection and obligations across the continent. Where necessary existing legal instruments should be revisited regularly to ensure that they are not in conflict with one another and that they offer complementary levels of protection and obligations within member states. In accordance with their legal systems member states should support the streamlining of these policies at subnational level to facilitate proper implementation at all economic levels. Intellectual

property laws should be revised to clarify that they do not generally impede the flow of data or data protection.

Actions

- Contracts that purport to give up digital rights, personal data protection and that inhibit competition should as a general rule be unenforceable. This can be articulated in data protection and competition regulation, which can also consider on a case by case basis whether pro-competitive effects of such contracts outweigh the anticompetitive effects.
- National law reform commissions or similar expert legal institutions should investigate and consider how to harmonise different branches of laws, regulatory regimes and supervisory authorities that deal with data;
- Member States should support the update or adoption of competition law frameworks and regulations that consider the challenges of analysing competition issues, designing remedies and enforcing their powers to safeguard competition in data-driven markets, as well as building capacity of competition regulators to implement these rules.
- Intellectual property laws should be amended to provide:
    - that if copyright applies to databases and compilations of data at all it shall apply only to the work of human authors that exhibit originality/creativity and that the copyright extends only to the original selection and arrangement of data in a database or compilation and not to the data itself;
    - that any copyright or other intellectual property right including trade secrets that enables control of data does not apply to personal data;
    - that any copyright or other intellectual property right including trade secrets that enables control of data is limited by the provisions of competition regulation and alternative rights that offer protection to local innovations not envisaged in current frameworks;
    - Adaptations to existing IPR regimes to leverage next frontier technologies, such as enabling AI to use data

5.3.4.1 Collaborating with regional and global governance processes

Regulation of digital and data economies is increasingly beyond the scope of individual national regulatory authorities (NRAs). Effective regulations require that regulators collaborate with regulators in their regions and globally to ensure the realisation of the internet as a public good, and its productive and rights-based use in the digital economy. Formal regulation should leave sufficient space for self-regulation, hybrid and collaborative regulatory models and oversight mechanisms for law enforcement. The range of tools and remedies at hand for regulators to explore is wide, from incentives and rewards through forbearance to targeted obligations. Regulatory instruments have expanded to cover regulatory sandboxes, ethical frameworks, technology roadmaps, regulatory impact assessments, multi-varied research and big data simulation to determine the most balanced, proportionate and fair regulatory response. AI, IoT and online disinformation are some of the complex issues waiting to be addressed (International Telecommunication Union, 2020).

5.3.4.2 Consultative and evidence-based regulations

In order to harness the expertise of stakeholders, regulation should also be the result of consultative multi-stakeholder processes focused on the public interest. They should also be evidence-based and contextual. Improved administrative data through better collection and analysis, and on which regulators can make decisions, would greatly enhance decision-making within agencies. This would also enable them to provide greater certainty to stakeholders within a flexible and adaptive framework, enhancing their credibility (World Bank & ITU, 2020).

Recommendations

In creating institutional arrangements Member States should clearly distinguish between the roles of the state as policy maker and the regulator, which should be sufficiently independent from the state and industry, so as to implement policy in the public interest and the service providers and platforms operators.

Regulatory institutions should be established on principles of autonomy, transparency, accountability to avoid state and regulatory capture. Regulators should undertake regulatory Impact Assessments at an early stage of regulation to implement best approaches that balance between regulation and economic growth. Regulators should publish performance of policy and regulatory efforts to improve regulatory strategies across states including public participation reports of emerging regulations Regulators also need to be self-financed or financed through parliamentary appropriation to enable financial independence. Regulatory decisions should be based on good data and harness private sector and civil society knowledge through public consultation. Competition and sector regulators should avoid instrumental competition regulation, by adopting dynamic efficiency rather than static efficiency models.

Actions

- Clearly distinguish between the roles of the state as policy maker and the regulator, which should be sufficiently independent from the state and industry, so as to implement policy in the public interest;
- Create or maintain competition authorities to deal with dominance in the market and concentration through mergers and acquisitions;
- Implement clear procedures for co-jurisdiction between sector and competition authorities to ensure the coordinated regulation of digital infrastructure and services sector and to avoid ‘forum-shopping’;
- Data regulators should collaborate at the regional and continental level to harmonise their frameworks, particularly in support of the AfCFTA.
- Those subject to decisions of regulatory authorities should have clear mechanisms of appeal and redress heard by a different body from the regulator, making the decisions in line with the rules of natural justice and fair administrative action.

5.3.5 Creating public value

Defining the problem

Having data without the human capacity, sufficient control, or incentives for value add, is much the same as not having data. These constraints apply to many African countries. There are also challenges in fostering a data-driven public sector. Data valuation is highly dependent on enabling regulatory and policy frameworks that facilitate obtaining useful data, enhancing human, institutional, and technical capabilities to create value from data,

encouraging data sharing and interoperability, and increasing legitimacy and public trust in the state to manage citizens' data in a responsible manner. Furthermore, the data infrastructure that enables an integrated data system is a key strategic asset for countries. The environment created by the interplay of elements in the data ecosystem and the nature of the relationships and non-linear processes between and within them, determine the interventions to create incentives for technology investments that are required to drive growth in the data economy. These conditions are shaped by the market structure, the competitiveness of the services that arise from it, and how effectively the market is regulated.

5.3.5.1 Public sector capacity

The public sector's digital and data capabilities are a key determinant of service delivery in many priority areas. Creating the conditions for data to be optimised in the public sector to meet the needs of citizens more effectively are necessary conditions of social and economic inclusion. However, there are multidimensional inequalities and overlapping policy inefficiencies that limit human and institutional capabilities to enhance a culture of digital entrepreneurship, foster inclusive digital innovation communities, and promote fair and equitable data ecosystems markets —where Africans with varying capabilities can work with frontier digital technologies and contribute to the data value cycle or participate in data value chains in a more inclusive manner.

For a data-driven public sector to materialise, the civil service needs to be revamped with leadership and political will to ensure that public servants at all levels are equipped with a basic understanding of how data can be used to enhance service delivery and policy implementation. Furthermore, a data-driven public sector requires a common approach and a data infrastructure architectural model that can address potential cross-industry, cross-application, and cross-platform integration and exchange of data and data-driven applications.

5.3.5.2 Public data curation

The public sector is mandated with managing key economic development data. This includes statistical data and economic indicators used for reporting purposes with multilateral institutions, and administrative data, such as Digital IDs. This is often anonymised and combined with other data across various use cases that range from commercial hyper-personalisation, such as credit worthiness, to public interest in social grants and disaster management.

Effective data driven value creation in the public sector requires a coherent transversal approach to understanding the need for data and how it can be used to enhance socioeconomic efforts and public service delivery. A lack of general consensus on data governance frameworks that are supplemented by the appropriate sector best practices (depending on the use case), can pose a significant threat to interoperability, open data sharing efforts, and create limitations on the extent to which governments can embrace practices to create value from data in the public sector. Facilitating interoperability is a critical issue, open data systems require a common approach and data infrastructure models that can address potential cross-industry, cross-application and cross-platform integration and exchange of machine readable data and data-driven applications. Data sharing and interoperability do not only depend on data systems, technical protocols, infrastructure, or governance —they also require leadership and political will for consensus around an approach to interoperability that is supported and adopted across various public sector mandates.

In the public sector data are often used to enhance the social contract and mitigate information asymmetries in policymaking, monitor intervention impacts, and service delivery, including deciding how government resources are allocated. Anonymised public data can be combined with other datasets for commercial use to lower market entry costs,

disrupt industries, enhance efficiency, and facilitate the development of innovations, products, information, and opportunities that can be available online, without the limitations of geographical and physical boundaries. However, institutions that curate public data face various challenges which are discussed below.

5.3.5.3 Ensuring quality and relevance of public sector data

There are several theories or models for studying data quality challenges. As a result, defining data quality determinants and relevance from a technical perspective are informed by a wide range of application scenarios such as the data availability, type of data, domain characteristics, and how and why the data is used, and/or collected, amongst others (Wang et al., 2019; Wook et al., 2021). For instance, in health research, a data quality assessment framework would consist of 30 or more data quality indicators, while for sensor data quality collected from IoT devices only two dimensions may be considered (Schmidt et al., 2021; Teh et al., 2020). Furthermore, the advent of big data analytics, including ML and technical capabilities beyond data science such as data engineering and data management, means that data is processed (cleaned) and can enhance the quality of the collected data, making it available for a wide variety of use cases (Wook et al., 2021, Svolba, 2019).

With education systems not adapted to the digital reality and therefore, poor STEM and ICT& digital skills means there is limited existing talent to fully make use of big data analysis techniques and data science to create value from accumulated or produced data [53]. Inadequate data curation and data sharing across the public sector inhibit the development of integrated data systems and the benefits associated with them.

Recommendations

- Given the breakneck pace of digitalisation, as the major steward of citizen's data, the public sector needs to be adequately resourced to leverage data to enhance public interests, in a manner that safeguards citizens. One way this can be done is through targeted training and knowledge co-creation initiatives with other international agencies— under-resourced institutions that curate public data already house existing analytical professions (statistics, quantitative economics, operational research and social research etc.) these existing resources can be upskilled and utilised to enhance data value creation in the public sector context.

- Member states should commit to a whole of government approach to using data across various policy priorities, public entities that curate various types of data must be given clear mandates and be resourced with technical, institutional, and human capacity. This can assist with ensuring they are accountable stewards of quality data that can be shared and repurposed in a responsible manner for multiple use cases.

- To promote trust in public data stewardship, sector regulators and public data stewards must ensure collaboration with industry stakeholders. As private sector data quality assessments are often beyond the public sector's control, industry data governance efforts are more suited for making laws and regulations that promote the use of high quality data. This is necessary to accommodate various use cases that require different data quality assessment indicators. These assessment guidelines should be done through multi stakeholder efforts—data governance must be

53

considered in the context of operational realities of various data use cases, across industries.

Actions

- Sector regulators and public data stewards must operate within specific guidelines on how data quality assessments should be implemented, depending on common use cases, algorithms, and type of data used, these guidelines can be informed by global best practices (including data and AI governance) but should be adapted to the context of African data use cases. Due to the exchange, combinations, strategic storage, and repurposing, required to create data value. An effective data quality strategy across the public sector should be informed by technical/practical/operational realities and should outline the roles, responsibilities, and mandates of various government agencies in collecting and maintaining high quality data in a manner that safeguards citizens.

- Member States need to participate in efforts to establish and adopt a normative framework for harmonised data standards and systems aimed at establishing national, regional, and international interoperability. These may include targeted human, technical, and institutional training interventions, sub-regional infrastructure projects, and REC regulatory sandboxes.

- A continental approach facilitates economies of scale to incentivise private investments in foundational digital infrastructure, including cloud based technologies. Regional harmonization of regulations for data governance could further reduce compliance costs and reduce uncertainty and operational risk for major ICT related infrastructure investments.

- Public institutions that curate data should be adequately resourced in order to contribute in multilateral fora regarding data and to be stewards of inclusive access and responsible use of data guided by appropriate industry technical and regulatory norms, standards, and best practices that underpin both the informational and economic characteristics of data in priority industries

5.3.6 Coherent sector policies to enhance data value

Defining the problem

Competition, trade and taxation policies are significantly intertwined. Competitive local data economies, for example, may increase data-driven services and trade openness can spur international digital trade and foreign direct investment (FDI) in domestic data economies. However, this also can reinforce the dominance of global oligopolies in domestic data ecosystems, creating trade tensions related to cross border data flows. Simultaneously data-driven digital business models may undermine domestic competition and reinforce market concentration as tax authorities struggle to quantify, value, establish, and track digital value chains due to characteristics such as third-party vendors and absence of physical presence as a basis for establishing corporate tax liability in the data-driven sector.

For Member States, collective action through a unified approach will more likely provide better outcomes that capture African contexts when addressing competition, trade, and taxation challenges in data markets.

5.3.6.1 Competition policy

Defining the problem

The dynamic characteristics of data-driven business models create challenges for implementing traditional competition policy tools, effective competition enforcement, remedies, and merger regulation in digital markets. Resolving these challenges requires pre-emptive market interventions and continuous collaboration with complementary policies such as consumer protection, trade, industrialisation and investment.

Competition policy should take into account not only the economic effects of data market structures but also the security and privacy effects, particularly in terms of avoiding concentration of data brokers or platforms, since this creates a risk of a single point of market failure. Thus enforcement of competition regulation and ex-ante regulation and policy design needs to be adjusted for the data economy.

5.3.6.2 Trade policy

Defining the problem

Digital systems no longer operate within clearly defined national jurisdictions. Trade policy reform is required to navigate increasing digital trade and e-commerce. Different geo-political influences, endowments, and institutional and human capabilities on the continent can affect unilateral approaches to digital trade and regional harmonisation efforts. The cross-border data strategy adopted domestically will require different institutional capabilities, can only be effective based on the existing data ecosystem endowments, will influence how data value will be created or extracted within and between African countries, and will determine who will benefit most from the data value cycle at a domestic and regional level.

Furthermore, “offline” factors such as physical road infrastructure, postal reliability, logistics and supply chain efficiency, amongst others are crucial enablers that facilitate both digital trade and ecommerce.

Services trade, cross border data flows and localisation

For digital trade to occur, data has to be moved across borders. While data accumulation can be a safe and secure way to manage data, hoarding data without means to use, exchange, or repurpose in a safe manner can also create underutilisation risks which may decrease efficiency and diminish other benefits of digital trade. Domestic data protection and regulations not only impact local business opportunities, they also affect intraregional trade and participation in the global data-driven digital economy.

While non-personal data are used and exchanged across borders, the importance of user-generated data and digital services as inputs in various industrial activities provides enormous scope to enhance exports of digital services. Services are also inputs in many manufactured products and in different data value chains. For this reason, three common general stylised data governance regimes for personal data cross-border flows have emerged, that range in openness, intervention required, and actors responsible. There are also variations of all the three stylised models depending on type of data and use case. Often, sensitive data such as personal data has more stringent cross-border data requirements than non-personal data. Data protection rules and standards can also be incorporated into sectoral regulations in highly regulated industries like health and finance that require more rigorous quality assessments and ethics considerations.

Choosing one stylised cross-border data protection regime over another should strike the balance between promoting equitable economic development and providing adequate data

safeguards. Member States need to understand the economic effects of different cross-border data governance regimes, based on their economic realities and development priorities. Furthermore, given the data infrastructure deficiencies for many African countries when it comes to storing and accessing massive amounts of data, while cloud data services are a more cost-effective alternative to setting up and running a physical data centre, they require certain factors that accommodate an environment for supply and consumption of cloud services. Ultimately, cross-border provisions for cloud computing services and data centres, such as data privacy, security, and restrictions on where data are housed (localisation requirements), need to be decided in consideration of broader economic development priorities.

The table below summarises the main pros and cons of each data governance regime, to aid policymakers with deciding the best approach to follow in the context of their sovereign and development priorities.

Three stylised approaches to governing cross border data flows

CROSS-BORDER DATA GOVERNANCE REGIME	DESCRIPTION	PROS	CONS	ASSUMPTIONS
Open transfers regime	• Relatively low a priori mandatory approval requirements, and voluntary private sector industry standards inform the free movement of data (eg. USA, APEC)	• Minimal regulatory burden allows for the greatest flexibility in the movement of data • Most suitable for digital services trade and data value creation • Privacy is a consumer right	• Risk of proliferation of standards across firms and jurisdictions, without guaranteeing any minimum standard for personal data protection • Requires, technical, human, and institutional capacity to monitor private firms and exercise ex post accountability • Limited data subject rights—lack of consent for personal data use	• Interoperable data systems and infrastructure • Human, technical, and institutional capacity to create value from data • Strong preconditions (enablers) to leverage the data-driven digital economy • Data subjects with digital capabilities to provide consent
Conditional transfers regime	• Consensus base, established regulatory data safeguards and overarching regulatory guidance from data protection authorities or international agreements (e.g GDPR)	• Offers more balance between data protection and the need for openness of data transfers for value creation • Encourages establishment of domestic data processing authority (DPA) • Clear guidelines and mandatory regulatory safeguards that once met allow for the free flow of cross-border data	• Based on strong data subject rights • Certain conditions need to be fulfilled ex-ante • Can perpetuate compliance burdens and digital trade bottlenecks	• Same as above • International collaboration and geopolitical influence to enforce ex- ante conditions
Limited transfers model	• Cross-border data flows are conditional based on government approval and localization requirements for domestic storage or processing of data (e.g China, Russia).	• Based on strong national security and public data control imperatives	• Stringent regulatory approval for international data transfers and may require explicit or implied data localization and mandatory storage	• Same as above

Source: Authors own interpretation summarised from Ferracane and van der Marel (2021), WDR (2021).

E-commerce

E-commerce platforms allow consumers to benefit from a wider variety of choices at more competitive prices. Strategies to enhance e-commerce cannot be formulated in isolation, since e-commerce intersects with a multiplicity of other issues including Digital ID, data governance, customs duties, cross-border data flows, cybersecurity, payments system interoperability, consumer protection,[54] competition, taxation, and standards, to name a few. Furthermore, improving e-commerce adoption requires addressing factors such as internet penetration, postal reliability, use of payments services (bank accounts or mobile money), and security of internet servers.[55] For Member States, collective action through a unified approach will more likely provide better outcomes that capture African contexts when

[54] Online consumer protection and product returns, consumer safety and supplier liability.

[55] https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf

addressing overlapping challenges that affect different government mandates at multilateral fora.
Trade agreements alone are not the appropriate cross-border data governance instruments. The current common approach to using trade agreements to govern cross-border data flows has not led to binding, universal, or interoperable rules governing the use of data across jurisdictions. However in the context of the AfCFTA, a harmonised, coordinated approach to addressing challenges associated with datafication domestically will contribute to better alignment with various overlapping intra-regional digital trade and ecommerce coordination efforts beyond the forthcoming e-commerce[56] and services trade protocols[57] in the strategy.

Recommendations

- To foster competitive, safe, trustworthy and accessible data ecosystems, competition authorities need to find coordinated, effective ways to regulate concentration while preserving the benefits that dominant firms offer in the context of different development needs across the continent. This includes ex-ante regulation of competition issues before they escalate in the market.
- Policy makers in the tax, competition and trade landscape will need to build human and technical capacity to address emerging issues beyond the traditional sectoral mandate that may affect data-driven markets;
- Member States must promote predictability and convergence of regimes across complementary policy areas in a manner that is mutually reinforcing. This needs to be done to navigate the emergence of new dynamic data-driven business models that can foster intra-Africa digital trade and data-enabled entrepreneurship. At the same time, policy makers should heed the two-way linkages between economic outcomes and data governance and carefully weigh the trade-offs.
- Member States should foster a coordinated, comprehensive and harmonised regional approach to global governance challenges associated with the global data-driven digital economy, such as:
    - cross-border collaboration in implementing competition policy instruments to address anti-competitive behaviour in data-driven digital markets;
    - encouraging data portability through regulation and other enabling activities;
    - the Organisation for Economic Co-operation and Development's (OECD) efforts to prevent tax avoidance in relation to data driven businesses;[58]
    - World Trade Organization's (WTO) agreements in data-enabled services and e-commerce;
    - establishing coordinated regional foundational data infrastructure and digital data systems development initiatives;

[56] The AfCFTA e-commerce protocol is an important tool to preserve the consolidated African market in the digital sphere, and preclude other arrangements which could potentially undermine the liberalisation and integration agenda. Guidelines are expected to be finalised in Phase III of AfCFTA negotiations.
[57] Phase II of AfCFTA set to address trade in services, intellectual property rights, investment and competition policy
58 https://www.oecd.org/tax/beps/

- strengthening human, technical, and institutional capacity to support data interoperability, value creation, and equitable participation in data economies; and
- contributing to international harmonisation of technical standards, ethics, governance, and best practices regarding data, big data analytics and AI.

Actions

- Member States should encourage dynamic policy and regulatory reform and experimentation (e.g. regulatory sandboxes at industry and REC level).
- Policy makers should heed the two-way linkages between economic outcomes and data governance and carefully weigh the trade-offs. Different state entities must endeavour to establish safe and responsible data-sharing frameworks that facilitate data demand, data interoperability, cross-border data flows, data value chains, and open data standards and systems within key priority sectors as assigned by the DTS. Where remedies are imposed they should be based on an economic assessment that accounts for long term impacts on incentives for investment and innovation.
- For data use to be efficient, inclusive and innovative, it will require collaboration between regulatory institutions across different mandates and coordinated market regulation (in interrelated policy areas such as telecommunications, Finance, competition, trade, taxation and data regulation).
- Competition authorities or related institutions will need to build human and technical capacity to address emerging competition issues beyond market concentration that may affect data-driven markets.
- Traditional competition tools such as guidelines on market definitions, assessing dominance, anticompetitive practices (e.g. abuse of dominance, coordinated practices, and abuse of buyer power), merger assessment, and theories of harm and designing remedies will need to be adjusted to incorporate the dynamism of data and characteristics of data-driven businesses.
- AfCFTA signatories will need to determine how the e-commerce protocol will operate alongside existing laws and policies, and will need to account for and support the objectives of the other protocols such as investment, intellectual property and competition policy (to be negotiated in Phase II). Develop and enhance public-private dialogue mechanisms to improve e-commerce-related policy making

5.3.6.3 Taxation policy

Defining the problem

There is an incongruence between where the profits of global platforms are currently taxed and where and how value is created from data within the digital economy. In Africa, most countries are mainly data markets for global platforms, with users contributing appreciably to the generation of platform profits, without a plausible value capture mechanism. Currently, Africa's data traffic is growing at an annual rate of 41% (UNCTAD, 2019) implying greater usage and adoption of the services provided by global digital platforms within the region. While there have been ongoing engagements by multilateral institutions, chiefly led by the

OECD's Inclusive Framework on Base Erosion and Profit Shifting (BEPS) (albeit not wholly inclusive for Africa with only 23 participating countries), a global consensus has not been reached for the different proposed options (Pillars One and Two) with respect to digital taxation.

Several African countries, reluctant to delay taxation of digital services or not aware of the benefits for their countries of the international reforms, are already implementing unilateral mechanisms. These include digital services taxes and equalisation levies based on significant economic (data) to capture some of the data value by taxing some parts of the digital economy within their jurisdictions. These mechanisms also include expanding sector-specific taxation on the telecommunications industry and taxing mobile money transactions and the usage of some over-the-top communications applications (OTTs) within the region, such as WhatsApp, Facebook, Twitter, Skype, and Instagram. While these taxes are driven to increase government revenues, the negative consumer impact has slowed digital access and inclusion (due to shifted consumer costs), and have restricted the right to free speech for citizens. On the supply side, the expanded taxes on the telecommunications sector impacts negatively on the profits of resident sector operators (with consequent negative implications for infrastructure investments critically needed within the resource-constrained region), while the data-based OTTs are largely untaxed locally (CTO 2020, ICTD 2020, RIA 2021, (CTO, 2020)) .

From a sovereignty and tax benefit perspective, every country is entitled to tax the profits of global digital platforms as long as they have an economic interaction with its citizens and residents (this is largely via sales of their personal data). However, despite having millions of its citizens and residents as users of data applications run by global digital platforms, African countries under the current international taxation regime do not have the required nexus for taxing the profits of these entities. While some of the platforms have some form of local presence in African countries, these subsidiaries are only set up as administrative support services and do not legally own the assets of these platforms (which are largely intangible and currently not included within the proposals of most apportionment formulas), and therefore do not receive any accruable revenues on the assets.

More so, the different tax propositions for the digital economy - which includes formulaic apportionments, application of Significant Economic Presence (SEP), and the use of indirect mechanisms such as value added tax (VAT) and more direct withholding tax (WHT) – all require access to transaction data, of which global digital platforms are currently not willing to share (especially in non-resident markets). Even in cases where some of this data is accessed, it will need to be verified and validated.

Recent legislative and policy measures introduced by select African countries, within the context of the several multilateral and unilateral efforts at taxing the digital economy, may not be conducive to either the creation of a single market or to accessing international resources to realise global public goods and meet some of the preconditions for a competitive data economy on the continent. Tapping into new sources of tax revenue might allow African countries to eliminate excise duties on social networking and data services reducing distortions to both the local market and the global tax system.

Recommendations

African governments need to increase economic activities within their jurisdictions that leverage digitalisation and datafication mechanisms, as enhanced productivity within this remit will amplify capacities for higher tax revenues. This process will require the development of more local data-based companies within the purview of the region's industrial policy. This pathway can help ameliorate fiscal compliance risks that are amplified within the current situation where a significant portion of public data within the region is captured and controlled by foreign data companies (Khan & Roy, 2019

Actions

- Member states should support the harmonisation of the tax regime for digital goods and services at the regional level, and alignment at the global level, which would mitigate the risks associated with small data economies markets being unable to generate significant value and compete in global markets to contribute to the scale and scope required for data-driven value creation and to generally limited tax bases.
- Complementarily, a public data fund coalesced by AU member countries could be set up in collaboration with the private sector to build the requisite infrastructure for extracting these transaction data, where the data can be retained as part of a regional data commons beyond just the remit of taxation purposes.
- Facilitating a public data fund will require African countries to digitalise their tax administration systems to enable more efficient assessment and collection of digital platforms taxes. A digital tax administrative system will enhance the capacity for tax registration, transaction data sharing with the National Tax Authorities and the exchange of tax obligation information with the digital platforms for compliance, while lowering operational costs.
- Member state should use the opportunity of coordination of taxation of digital services for a single digital market to tap into new sources of tax revenue that might allow them to eliminate regressive and fiscally counterproductive excise duties on social networking and data services and reduce distortions to both the local market and the global tax system.

5.4 Data Governance

For data governance policy to be effective it should encourage an ecosystem where there are multi-stakeholder efforts to improve data access and use. It should also encourage the repurposing and combination of data in a manner that limits harms and risks associated with the processes of datafication while ensuring that a wide variety of data will be used to its greatest economic and social potential. Some of these policies involve making data available while others restrict the flow of data (Macmillan 2020).

5.4.1 Data control

Facilitating control of data for firms and government is an important mechanism for extracting data value (Carrière-Swallow & Haksar, 2019; Couldry & Mejias, 2018; Savona, 2019). Policy helps to both limit the manner in which control can be exerted, but also encourages mechanisms for control that align to the strategic objectives of a data policy. An important role for policy is helping to ensure clarity in terms of control for the assignment of obligations and responsibilities (Carrière-Swallow & Haksar, 2019; Zuboff, 2018).

5.4.1.1 Data sovereignty

Data control can also be understood at a national level in relation to data sovereignty (Ballell, 2019). Data sovereignty draws on the concept of the sovereign nation state and refers to the view that data that is generated in or passing through national internet infrastructure should be protected and controlled by that state ((Razzano et al., 2020). In the digital context, it can be understood as a subset of cyber sovereignty defined as the subjugation of the cyber domain (which is global by definition) to local jurisdictions (Polatin-Reuben & Wright, 2014). Two approaches of weak and strong data sovereignty, exist. Weak data sovereignty refers to private sector-led data protection initiatives with an emphasis on the digital rights

aspects of data sovereignty. Comparatively, strong data sovereignty favours a state-led approach with an emphasis on safeguarding national security (Polatin-Reuben & Wright, 2014).

In general, the transfer of personal data to another country is allowed only under certain conditions, for instance when another country has a law that requires sufficient safeguards (including privacy and security) for the processing of personal data. States often exercise data sovereignty for the protection of the rights of their citizens, such as through data protection regimes that regulate cross border data flow to protect the rights of data subjects, often through agreements setting data protection standards and reciprocal protection of exchanged data. While sufficient legal standards are necessary for reciprocity so is the practical ability of states to enforce mutually agreed standards. Ensuring sound data governance practices is a foundational step for realising data sovereignty.

5.4.1.2 Data localisation

Defining the problem

While data localisation is often seen as an expression of state sovereignty, as a possible policy option data localisation needs to be assessed on a cost benefit basis. This policy choice may present a practical challenge. While data localisation is sometimes motivated by the need to protect data subjects, data localisation can be applied to non -personal data. This is why it is essential data localisation is read in the context of control, in order to emphasise in policy the importance of supporting mechanisms that can facilitate the act of sovereignty. Data localisation involves the artificial erection of legislative barriers to data flows such as through data residency requirements and compulsory local data storage (Cory, 2017). Strict data localisation rules requiring the storage of all data locally, and not merely a copy, renders such data susceptible to security threats including cyber-attacks and foreign surveillance. Some African countries face acute technological capacity constraints so that localisation capacity demands may vastly exceed national data centre capacity. Concomitantly, requirements for duplicate copies of data may place undue financial obligations on local companies.

Recommendations

- Member States should prioritize politically neutral partnerships that take into account their individual sovereignty and national ownership to avoid foreign interferences which may negatively affect the national security, economic interests and digital developments of AU Member States.
- AU Member States have the right to formulate digital and data rules in line with their priorities and interests notably to protect the information security of the state and its citizens, and to prevent third parties from unfairly exploiting resources and local markets.
- Bilateral and multilateral agreements need to be established to exert domestic sovereignty and control, and recourse avenues for infringements are required.
- Localisation needs to be evaluated against potential harms to human rights.
- Data localisation requirements require data specificity. Data localisation solutions have been strongly articulated within sectoral (vertical) data silos across different jurisdictions; for instance, Nigeria instituting certain forms of financial data localisation, Australia prescribing forms of health data localisation, etc. This is an area in which specificity is strongly required both for facilitating broader flows as far as is conducive with policy imperatives like the Africa Free Trade Area, but also for clarity which can help minimise

the costs for local businesses and innovators and reduces the risks of unintended consequences.

- Data policy requires clarity not just through specificity, but also in relation to data categorisation which can allow Members to exert sovereignty through the establishment for instance of security classifications, or specific levels of data sensitivity. These should be consistently applied across data (and information) policy.
- Data infrastructure development should be explored as a mechanism for exerting control, but must be contextualised in consideration of environmental impacts, safety and security infrastructure, duplicated costs for local data communities, and overall costs.
- Public sector capacities should be invested in to inform domestic and effective data control initiatives.
- Data subject rights should be designed and expressly provide for effective personal data control. Data trusts and stewardships should be explored as another form of effective personal data (and other data) control.

Actions

- Data protection authorities (DPA) need full empowerment which includes remit on data sovereignty.
- DPAs are encouraged to adopt international and regional cooperation practices taking note of different stages of implementation and enforcement across Member States.
- Risk assessment and multi-stakeholder engagement should be used to design data localisation solutions in policy by drafters, which includes civil society participation.
- Data infrastructure policy should be aligned with data control imperatives by policy drafters, but must consider cybersecurity, personal data protection, environmental risks and cost.
- Public administration and investment policy should align with data control capacities as a priority.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation.

Mechanisms for exerting data control
There are mechanisms for exerting data control such as through data trusts. Data trusts and/or stewardships are alternative forms of discrete governance solutions in the context of data. A legal trust is a legal instrument used to manage property, both corporeal and incorporeal. A trust allows someone to hold assets (which they do not own) for the benefit of the trust beneficiaries. The person who holds the assets has been authorised to do so and owes the beneficiaries of that trust a fiduciary duty to act responsibly in the management of their assets. This traditional legal structure has been posited as a way of managing collections of data on behalf of groups, and facilitating mass data sharing in situations where licensing or open data models might not be feasible as a means of fostering innovation through facilitating fair access (Stalla-Bourdillon et al., 2019).
The Open Data Institute defines data trusts as providing "…independent, fiduciary stewardship of data" (Open Data Institute, 2018). The addition of the fiduciary element to

the definition (as opposed to merely defining it as a form of legal trust) was added as being an essential element of responsibility and obligation, which forms an important foundation to the concept (Open Data Institute, 2020). In addition, it can include privacy-by-design solutions within the architecture of any mechanism designed to facilitate the trust, thus in ensuring privacy in substance and process (Stalla-Bourdillon et al., 2019). While data protection laws might create standards for how a person's data can or cannot be processed, outside of consent or recourse for violations, the mechanisms for persons to act in relation to their data is limited - thus, data trusts help to facilitate realising data control. Data trusts provide a data subject with a mechanism through which they can provide (or 'share') their data, while also removing from them the sole responsibility for 'ensuring' data protection compliance by both public and private sector actors through the establishment of a fiduciary relationship.

5.4.2 Data processing and protection

Defining the problem

While data control principles help to outline delineation and obligations in respect of both personal and non-personal data, data processing seeks to outline the policy guidelines for the processing of personal data, as discussed earlier. Regulation of non-personal data is determined by data categorisation and specific access regimes.

These forms of guidance are important as a mechanism for realising privacy and data protection. Personal data processing is a critical component of data governance and fostering a trust environment. The building of trust is understood as a necessary part of the fostering of a sound data and digital economy. By constraining process limitations to personal data, such constraints need not impede the data flows for digital trade; but to ensure such lack of impediment requires consistent data policies across the region based on shared, but flexible, principles (United Nations, 2017).

Data subject rights, as an aspect of personal data processing, also offers ancillary benefits for helping to ensure data integrity and quality.

A privacy-by-design approach can be taken when developing digital technologies and systems by which privacy is incorporated into technology and systems by default during the design and development process (Cavoukian, 2009). For instance, it may entrench minimality in its data collection or automate rigid de-identification. It means a product is designed with privacy as a priority, along with whatever other purposes the system serves. This design should incorporate a particular understanding of how data subjects engage with products, and their capabilities for asserting their privacy.

De-identification techniques, including anonymisation and pseudonymisation, can facilitate some uses of data while providing at least partial data protection. Pseudonymisation can be accomplished through use of a signifier or mask that can only be connected to an identifiable individual through additional data. While both anonymisation and pseudonymisation may enable both private service providers and the public sector to make greater use of data they are reliant on the current state of technology and mathematics. As new mathematical approaches are developed and computer processing power increases data that was deemed de-identified may become identifiable. While data protection regulations often require de-identification these techniques are insufficient without strong legal rights for data subjects and a regulator with capacity to enforce data protection.

Recommendations

- DPAs must be established that are independent, funded and effective. Additionally, as a method of ensuring effectiveness, accountability metrics are crucial for helping a DPA have a clear scope. Lawful data processing frameworks must be established which include clear deterring penalties to ensure compliance. They must cover all relevant data processing actors.
- Personal data risk assessment should be obliged in the deployment of personal data technology development.
- An important sub-principle, which must be actioned with data processing frameworks for public and private stakeholders, is that of minimisation. The minimisation of personal data collection is one of the most effective mechanisms for mitigating against data subject risks and harms.
- Codes of Conduct should be explored for promoting data and sector specific needs. Such Codes, approved by the relevant DPA, can provide sector and industry expertise into managing the real risks and harms that may be associated to processing, and ensuring best practice in the management of those harms. It can also help to consider the sectoral exceptions which may be required for a constructive data economy to thrive, but also feed into a broader Sustainable Development agenda, such as through the ready facilitation of research (in health, or other social development arenas).

Actions

- Data processing frameworks should be established in partnership with all relevant multi stakeholder partners but driven ideally by the DPA. These should align with the following principles: consent and legitimacy; limitations on collection; purpose specification; use limitation; data quality; security safeguards; openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity.
- DPAs should be established as a matter of urgency alongside national legislations on personal data protection. .

5.4.3 Data access and interoperability

Defining the problem

Data access and accessibility is understood both in terms of reactive forms of access facilitated by laws and regulations, as well as through proactive forms of data access (such as through open government data) (Open Data Charter, 2015). Accessibility also implicates sharing of data across agents or departments, an important benefit of data's non-rivalrous nature. Yet this requires interoperability between these different agents (Jones & Tonetti, 2020). In the context of competition, data is not simply portable in a way that can facilitate scale effects easily between firms (Rinehart, 2020). Requiring forms of data portability remains a key cited regulatory strategy for facilitating competition and consumer benefit, though the realities have not yet been established as definitively beneficial ((Mitretodis & Euper, 2019; Rinehart, 2020). From a privacy perspective, outside of just interoperability changes, the nature of big data collection means that data portability implicates other users' privacy (Nicholas & Weinberg, 2019).

Recommendations

- Open data standards should be prioritised in public data creation and maintenance. The creation of data to these standards does not preclude overlaid mechanisms for control or limiting access in defined data categories for compelling purposes.
- Data portability should be supported. Data portability can be a form of data subject right, defined as the right of the data subject to obtain data that a data controller holds on them, in a structured, commonly used and machine-readable format, and to re-use it for their own purposes. Portability can be facilitated through a policy on data portability in public sector data, and through the establishment of specific data portability rights in consumer contexts.
- Data partnerships (including options like databanks) should be prioritised as mechanisms for advancing quality and privacy-preserving open data.
- As a method of trying to facilitate specificity, data categorisation can be a method for ensuring cohesion within data processing frameworks within processing allowances, and security principles. The categorisation referred to here is not such as the sectoral typologies considered more broadly, but rather as a specific mechanism for realising particularly forms of risks that align to data and information types, and might include sensitive categories (such as children's data), security classifications of relevance, as compared to forms of data already in the public domain.
- Restrictions on processing need to be clearly articulated and limited, in order to not interfere with low risk processing that might be increasingly central to the training of AI through large-scale data processing.

Actions

- Member States should establish an open data policy which sets open standards for the production and processing of data, so that when decisions are made to open the data, the high costs of ensuring it is usable and manipulatable are avoided.
- Sectoral laws and codes of conduct from DPAs should be reviewed to ensure lawful data access in conjunction with the data policy.
- DPAs should have a dual access to information and privacy function.
- Multi-sectoral open data initiatives should be implemented on priority data sectors like health, research and planning.

5.4.4 Data security

Defining the problem

Data security includes the set of policy, norms, regulations, legislation and practices to protect the confidentiality, integrity, and availability of data from unauthorised access, corruption or theft, throughout the entire lifecycle of data. These fundamental principles of data security also define the three main areas of accountability of information security. The concept of data security encompasses many aspects, from the physical security of hardware of data centres and storage devices to administrative access controls, as well as the logical security of networks, software, and applications. It also includes organisational procedures and policies.

Confidentiality, integrity, and data availability, from a regulatory perspective, depend on national cybersecurity policies and legislation. The security of data (including confidentiality, integrity and availability) also does not depend on the physical location of the servers which

are hosting such data. Rather, it is a function of the normative rules - including norms, policies, regulations, laws and protocols (such as data standards and technical interfaces), and the implementation of technologies and security measures (such as encryption, firewalls and access controls) - that are put in place by public or private service providers in the way that they store, access, share and use the data.

Increasing data security legislation and technical measures may both improve confidentiality, integrity and availability (positive security) as well as undermine fundamental freedom and rights of privacy, dignity, and safety online (negative security). For example, to protect users' data safety and security, some countries may impose restrictions on data sharing and transfer by enacting cybersecurity legislation. These can be barriers to the free flow of data. From a cybersecurity perspective, some states may believe that data is more secure if it is stored within national borders. States may erroneously refer to it as principles of data sovereignty, while these measures are simply forms of data protectionism and data localisation.

A principle that is difficult to uphold with regards to data security is that of transparency. While countries continue to witness an increase in the number of attacks being reported to law enforcement, improvements in this area have been driven almost entirely by data protection regulations, and reported incidents are primarily data breaches. On the other hand, increasing transparency on data security includes both technical aspects such as reporting on zero-day vulnerabilities and adherence to international cybersecurity standards, as well as policy aspects related to the assessment of cyber capacity maturity. Transparency on data security has the potential to improve technical and procedural defence mechanisms against attacks and to strengthen collaborative practices based on information sharing.

Recommendations

- Member States should develop national cyber Security policies as well as necessary legal and technical measures to sustain trust in their digital space.
- Member States are encouraged to co-operate regionally to develop cybersecurity standards to be met in both the public and private sectors to increase regional economic growth.
- Data policies should align with cybersecurity and cybercrime policies, and legislation dealing with cybercrime should respect human rights.
- A joint sanction regime for cyber-attacks should be established.

Actions

- Member States, who are yet to develop cybersecurity measures, should immediately develop cybersecurity plans and streamline them within government governance structures to promote robustness and reduce vulnerabilities.
- Cybersecurity institutions like CSIRTs should be incorporated into data policy development.
- Data processing roles as a form of security protection should be specified in policy by policymakers.
- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation, and could be supported by DPAs.

5.4.5 Cross-border data flows

An increasingly important issue regarding international and regional trade is the cross-border transfer of personal and other data (Deloitte, 2017). In the African context, international and regional frameworks that facilitate cross-border transactions and personal data flow across countries are essential for the creation of common markets and particularly for the realisation of the African Free Trade Area. Cross-border data transfer of personal data, in particular, is shaped by the data sovereignty approach that a country wants to pursue, which refers to the legal principle that information (generally in electronic form) is regulated or governed by the legal regime of the country in which that data resides. As noted, this concept is challenged by the modern reality of data movements. Critiques of the supposed ' data flows' narrative and the extent of its benefits for digital dividends in development should however be acknowledged, as should recognition that significant amounts of data flows actually occur horizontally within firms, rather than between firms (UNCTAD, 2021).

It is also worth mentioning the common position that the transfer of data is dependent on whether the receiving country has an adequate level of protection (Razzano et al., 2020). However, what amounts to this 'adequate' level will frequently be determined by a country's Data Protection Authority, or similar. Thus, in the absence of a data protection law in the receiving country, the transfer of personal data cannot be subject to proper regulation unless the law of a country forbids transfer of data except to a country with an adequate level of protection, or through the establishment of bilateral obligations through contracts between the transferring parties.

The reality is that broad limitations on cross-border data transfer could result in business opportunities lost, and reduce the ability of an organisation to trade internationally, leading to a reduced geographical footprint and loss of market competitiveness. Data regulation that is synchronous with regulations in other jurisdictions contributes to mutual trust and lays a foundation for a trusted exchange of data, including (but not limited to) personal data. In this sense, personal data protection regulation enables and improves trust and trade in the cross-border movement of persons, goods and services (Information Society, 2018).

Recommendations

- Data protection frameworks should provide minimum standards for cross-border data flows.
- The establishment of norms and standards should expressly ensure reciprocity as a central principle for permitting cross border flows.
- Data specificity should be prioritised to avoid unintended restrictions on productive data sharing.
- Law enforcement considerations should be incorporated in the policy-making process.
- To ensure effective cross-border resolution, a degree of capacity must be ensured across agencies.
- Members of the African Union should rigorously define a framework and modalities to regulate cross borders data flows, and identify the African entity and persons entitled to manage this system.

Actions

- DPAs should ascertain minimum standards for data transfer.

- Capacity-building in relation to data protection, cybersecurity and institutional data governance in relevant agencies should be assured through policy and asset allocation, and driven ideally by DPAs in conjunction with educational facilities, and government skills programmes and units.

5.4.6. Data demand

While there are significant data and digital economy recommendations that relate to helping create a broader data ecosystem, there are also specific policy interventions to be pursued in relation to demand-side data stimulation. Data users may be the public sector, private companies (of different sizes), and also individual users and citizens. However capacity needs to be developed across these profiles to stimulate demand for data, data cultures and innovation. The role of policy in fostering the productive use of data across stakeholders is facilitated by the preceding policy areas, but may also require more specific considerations. This is especially the case given that the data reality for many local actors within the data ecosystem is one of data scarcity, rather than saturation.

Recommendations

- Data communities should be prioritised in innovation policy. These communities require domestic policy incentives and support, including the active promotion of data hubs and other forms of community innovation that can help engender data competencies and data cultures, as should civil society actors more broadly.
- Regulatory provision for data management should include provision for regulatory sandboxes to encourage local data development.

Actions

- Data communities should be incorporated in data policy-making processes by policy makers.
- Data communities should be drawn into the establishment of open government data initiatives by departmental implementers.
- Universities should be included as relevant policy stakeholders to help establish the "knowledge-base" from which the local data economy can draw sufficient scientific and technological knowledge.

5.4.7 Data Governance for Sectors and Special Categories of Data

Certain categories of data, and certain specific sectors require tailored data governances that take into account the particular issues that affect that category or sector. Categories such as health data or children's data are not the same as sector specific typologies such as financial data but both may require distinct treatment. However special treatment creates a threat of data silos that render data less useable and may raise compliance costs, especially if there are incompatible regulations or requirements. Special treatment is sometimes necessary but should be in harmony with general data governance and this policy framework.

A key recommendation of Data Access and Interoperability is that types of data that require special consideration be identified, and clearly specified so that special access and other requirements in respect of that data integrate with general data rules. As discussed under Data Localisation clearly specified types of data are sometimes subject to data localisation requirements in pursuit of policy objectives peculiar to the type of data. In the Data

Processing and Protection recommendations it is recommended that codes of conduct, subject to approval by the national DPA, can be used for sector specific requirements.

Recommendations

- Members should avoid special data regimes that are not integrated into national data regimes and that do not incorporate the principles of good data governance.
- Governance mechanisms and policies should enable the development of category and sector specific data governance for children's data, health data and other kinds of sensitive data or sector specific data that warrant distinct treatment through processes that are in accordance with the principles in the framework.

5.5. International and Regional Governance

At a transnational and continental level - particularly to provide capability for cybersecurity and to address data protection concerns associated with the changes in data economics - cooperation between countries is of increasing significance. The scope of cooperation needed includes dialogue between governments, collaboration with the private sector, and effective, integrated processes to investigate and prosecute cross-border breaches. A global trust architecture that accounts for the limitations of existing national or otherwise fragmented systems is essential to secure a digital economy and digital inclusion (African Development Bank 2019).

Certain international and continental-wide initiatives serve as a foundational step for precipitating implementation.

For instance, the African Union and regional initiatives on digitally encoded genetic data[59] and geographical and environmental data respectively. The African Union Commission will ensure harmony between these initiatives and the ongoing data policy work[60].

Recommendations:

The African Union with support of sister panafricaine organisations should:

- Facilitate collaboration between the various entities dealing with data across the continent through the establishment of a consultation framework within the digital ecosystem community to safeguard the interest of each actor.
- Strengthen links with other regions and coordinate Africa common positions on data related international negotiations to ensure equal opportunities in global digital economy.
- Support the development of regional and continental data infrastructure to host advanced data-driven technologies (such as Big Data, Machine learning and Artificial Intelligence)

59 While the category of digitally encoded genetic data includes the genetic data of humans, where these are identifiable individuals this should be regarded as sensitive data and dealt with as required by the Malabo convention. But there are other kinds of digitally encoded genetic data that require specific/special treatment that are neither sensitive data nor even personal data. These include demographic genetic data, and the genetic data of organisms other than humans. The African Union is currently engaging with other countries who are parties to the Convention on Biodiversity (CBD) to ensure that digitally encoded data should be treated as 'biological resources as that term is used in the CBD. The convention states that biological resources "includes genetic resources, organisms or parts thereof, populations, or any other biotic component of ecosystems with actual or potential use or value for humanity". The convention governs both access and benefit sharing to both enable research and to require that people who are custodians of biodiversity share in the benefits of that research. Applying the rules of the convention will enable beneficial data flow while also ensuring that Africans benefit.

60 The Regional Data Strategy for Marine and Coastal Areas Management in Western Africa promotes more sustainable management of natural resources through mutual sharing of data.

and the necessary enabling environment and data sharing mechanism to ensure the circulation across the continent;

-

5.5.1 Continental data standards

As a means of facilitating cross-border cooperation, it is important to achieve consensus on data standards, which is an integral consideration for advancing interoperability. These multistakeholder forms of consensus should reference the work done through the International Organization for Standardisation, and other forms of international consensus achieved in specific sectoral contexts. However, while international standardisation is important for competitiveness, it should be noted that these international standards may not be sufficient for the region's needs. This is demonstrated, for instance, in language challenges found in the context of spatial or geographical data.

Recommendations

- Consensus on data standards should reference the work of the International Organization for Standardisation, amongst other relevant forums;
- However, standards need to be set with specific reflections on contextual factors impacting the continent.

Actions

- Establish or empower a mechanism within the African Union for centralising and empowering regional engagements on data standards.

5.5.2 Open data portal and other initiatives

There are important open data initiatives already occurring centrally which should remain supported in the name of a sound regional data economy. These include the African Development Bank's central open-data portal (https://dataportal.opendataforafrica.org/). Besides this, institutionally driven initiatives (as in https://www.datafirst.uct.ac.za/dataportal/index.php/catalog/central/about) and volunteer-driven communities (such https://africaopendata.org/).

5.5.3 Continental instruments

The broad range of existing relevant instruments are outlined in section 4. However, there are two specific areas that need to be highlighted.

Cross-border data flow mechanism

There is an opportunity to leverage this framework to begin collaboration towards a regional cross-border data flow mechanism, facilitated by an overarching instrument, such as those by the OECD and ASEAN.

AU Convention on Cybersecurity and Personal Data Protection

It is recommended that the AU Convention be ratified as soon as possible to serve the foundational step for the harmonisation of data processing. Additional protocols to the Convention should also be explored to reflect changes since the original drafting.

African Continental Free Trade Agreement

The AfCFTA provides an opportunity for co-operation on a number of important aspects of the Data policy framework, most saliently in the development of the agreements on competition, intellectual property and investment.

Recommendations

- Promote and facilitate data flows within and among AU Member States by developing a Cross Border Data Flows Mechanism that takes into account Africa context namely the different levels of digital readiness, data maturity as well as legal and regulatory environments.
- Facilitate data circulation across sectors and cross borders by developing a Common Data Categorisation and Sharing Framework that takes into account the broad types of data and their different levels of privacy and security.
- Work in in close collaboration with national authorities in charge of personal data protection of AU members, with support of the African Network of Authorities (RAPDP), to establish a coordination mechanism & body that oversees the transfer of personal data within continent and ensures compliance with existing laws and rules governing data and information security at national level;
- Enable data sharing and enhanced interoperability among AU Member States and other AU mechanisms including the African Union Mechanism for Police Cooperation (AFRIPOL).

- Work towards building a secure and resilient cyberspace on the continent that offers new economic opportunities through the development of an AU Cyber Security Strategy and establishment of Operational Cybersecurity Centres to mitigate risks and threats related to cyberattacks, data breaches and misuse use sensitive information.

- Establish mechanisms and institutions , or empower existing ones , within the African Union to build capacity and render technical assistance to AU Member States for the domestication of this data policy framework
- It is recommended that the negotiation of the competition chapter of the AfCFTA should set minimum standards to ensure that putatively proprietary non-personal data is accessible to innovators, entrepreneurs, and others in the value chain for the purposes of encouraging competition across the continent.
- Members of AfCFTA should consider including provisions in the competition chapter that mandate competition authorities considering market structure issues to also consider the security and privacy effects of market structure. This is important to avoid the concentration of data brokers or platforms both nationally and regionally, since this creates a risk of a single or few points of failure with far reaching consequences.
- Members of AfCFTA should also consider including provisions in the intellectual property chapter of AfCFTA that clarify the status of data in respect to intellectual property, in particular:

    - that if copyright is extended to databases and compilations of data that it only applies when databases and compilations are created by human authors and exhibit originality and that the copyright extends only to reproduction of the original selection and arrangement of data in the database and not to the data itself;
    - that any copyright or other intellectual property right including trade secrets that enables control of data does not apply to personal data; and
    - that any copyright or other intellectual property right including trade secrets that enables control of data is limited by the provisions of competition regulation.

Actions

- Member States should ratify the AU Convention on Cybersecurity and Personal Data Protection and develop additional protocols, as required, to reflect changes since the original drafting ;
- establish, or empower, a mechanism within the African Union for centralising regional engagements on data standards;
- once adopted, alignments with the AfCFTA process should immediately be explored;
- include data in negotiations on the AfCFTA chapters on competition and intellectual property; and
- agree on common and consistent criteria for assessing adequacy in the levels of protection of personal data across the continent to facilitate and enable trans-border transfer of data and standardise protection.

5.5.4 Continental and regional institutions and associations

Regional institutions and associations create a central mechanism for creating a unified regional voice on data issues. Many associations already exist, and ensuring the implementation of this framework speaks to existing associations is a priority recommendation. Continental and regional bodies are particularly important due to the cross-border nature of data flow required to benefit from data.

Regional economic and development communities

The Regional Economic Communities as building blocks of the African Union can assist member states to create capacity, domesticate data policy and reach consensus on harmonisation of data policy, participate in standards making, and enable data flow.

Human rights adjudicators

The African Court on Human and People's Rights, the East African Court of Justice, and the ECOWAS Community Court of Justice provide fora and skilled capacity to adjudicate complex disputes on privacy and equality, which are relevant to personal data protection and the use of data to unfairly discriminate.

The SADC Tribunal, once recapacitated, could also offer a forum for data disputes, albeit within a more limited mandate. Continental and regional adjudication mechanisms are best placed to resolve cross-border data disputes

African Network of Data Regulators

Empowering DPAs and improving the level of enforcement of legislative and regulatory frameworks at national level significantly assist individual's enjoyment of digital rights. An avenue for this capacitation is through the promotion and support of existing associations, such as the African Network of Data Protection Authorities.

ICT regulatory authority associations

There are existing ICT associations such as the Regional Association of Regulators (ARTAC, WATRA, CRASA and EACO) that stand as important mechanisms for peer learning on cross-border association. They can also facilitate collaboration and knowledge sharing as cross-border instruments and standards are explored.

Sectoral associations

Sectoral associations like the African Tax Administration Forum will be needed to help realise data economy recommendations areas in particular. Given the importance of digital identity within the data economy, the Association of National Registrars is also important.

African Competition Forum

The African Competition Forum (ACF) describes itself as "an informal network of African national and multinational competition authorities". The ACF can create capacity for competition authorities to better regulate data issues.

Recommendations

- Strengthen regulatory cooperation and knowledge sharing among African countries and regions by building capacities of the African Network of Data Protection Authorities and the Regional Association of ICT Regulators.
- Existing continental and regional adjudication mechanisms should be explicitly empowered to deal with data issues that are implicated in digital rights and data rights, and cross- border data disputes.
- African tax authorities should collaborate through the African Taxation Administration Forum (ATAF) to develop an African position to more effectively represent common interest in international taxation reforms process such as BEPS.
- Establish an Annual Data Innovation Forum for Africa to serve as a platform for multi stakeholder discussions, facilitate exchanges among Countries and raise awareness of Policy makers on the power of data as the engine of today digital economy.

5.6. Implementation Framework

5.6.1 Phases of Implementation Framework

It should be noted that while the activity areas below are identified as phases, their fulfilment is not strictly linear. Particularly, phases 2 and 3 are considered to be concurrent processes, which can occur alongside domestication activities. The implementation framework should be read in conjunction with the stakeholder mapping outlined in 5.6.2

	Activity	Description	Lead Responsibility
PHASE 1: ADOPTION OF THE FRAMEWORK			
A	Member states adopt Framework		Members
B	Design of Monitoring for Framework	High-level monitoring framework established,	AUC
C	Establish or empower a mechanism within the AU for centralising regional engagements on data.	Activities to include implementation support, coordination on data standards, and other specific areas enunciated in the recommendations requiring regional collaboration.	AUC
PHASE 2: ESTABLISHING BUY-IN/OWNERSHIP			
A	Assess Continental Framework	Ensure alignment with continental instruments.	AUC, RECs , AUDA-NEPAD Smart Africa
B	Engage Continental Structures	Engage associated structures on potential areas of collaboration in implementing the framework.	AUC
C	Assess International Frameworks	Focusing on principles, explore alignment with frameworks of international structures.	AUC
D	Engage International Structures		AUC, AU Member States
PHASE 3: CONTINENTAL SUPPORT FOR MEMBER STATES TO MEET PRECONDITIONS			
A	Develop broadband infrastructure and regulatory frameworks	Broader policy implementation initiated in relation to the enabling data environment, domestically.	RECS, AUDA-NEPAD, ATU ,PAPU , SMART AFRICA
Phase 4: Domestication			
A	Multi-stakeholder engagement	Leveraging the Policy Framework, engage domestic actors.	Members, private sector, civil society,
B	Establish multi-stakeholder buy-in	Reflecting on the stakeholder mapping under Phase Two*, ensure policy alignment.	Members
C	Domesticate instrument	Develop Legal and Regulatory Frameworks, establish data regulators and data governance systems	Members

D	Budgetary framework	Allocate resources for implementation	Members
PHASE 5: COLLABORATION			
A	Engage Decision-Making International Fora	Engage rule-making fora on data standards and rules (see stakeholder mapping).	AU Member States
B	Monitoring of member implementation		AUC , RECs, AUDA-NEPAD, Smart Africa
C	Drive awareness on the centralising continental mechanism on data.	Accept direct requests for assistance	AUC, Regional Institutions
D	Participate in continental activities	Participate in the continental activities outlined in Section 10.	Members

5.6.2 Stakeholder mapping

A cursory stakeholder mapping is provided to facilitate implementation, particularly at Phase 2, Phase 4 and Phase 5.

DESCRIPTION	SUB-TYPES	PURPOSE
INTERNATIONAL		
United Nations	International Telecommunication Union, UN Department of Safety and Security	Alignment of development policy
Multilateral Organisations	Organisation for Economic Co-operation and Development, World Bank	Alignment of economic policy
Internet Governance Structures	Internet Governance Forum, Internet Engineering Task Force, Internet Corporation for Assigned Names and Numbers	Alignment of digital and Internet policy
International Standards	International Organization for Standardization	Alignment of data standardisation
Multilateral Organisations (sectoral)	World Health Organisation, World Trade Organisation	Alignment of sectoral components of policy
REGIONAL		
Regional Economic Communities	ECOWAS, SADC, , EAC, ECCAS, COMESA, IGAD, CEN–SAD , UMA ,	Alignment of economic and development policy
Internet Governance Structures	AFRINIC, African IGF	Alignment of digital and Internet policy

Regional Community (regulatory)	Network of African Data Protection Authorities, Other Regulatory Associations, African Tax Administration Forum	Cross-border policy alignment
Regional Community (sectoral)	African Development Bank	Alignment of sectoral components of policy
DOMESTIC		
National Departments	Telecommunications, Justice, International Cooperation, State Security	Policy alignment
Statistical Agencies		Capacitation
Regulatory Authorities	Data Protection, ICT Regulation, Competition	Implementation
Firm-level	Data governance committees	Capacitation, multi-stakeholder engagement

Recommendations:

Following the endorsement of the Continental Data Policy framework by AU Organs , the AU Commission in collaboration with regional institutions and relevant stakeholders will develop an Action Plan to guide the implementation of the framework that takes into consideration digital sovereignty of states as well as the different levels of development, vulnerability of populations and digitization within AU Member States namely aspects related the gap in ICT infrastructure and lack of cybersecurity policies and legislations.. The action plan (short, medium and long term) will identify roles and responsibilities and emphasize the key priorities and immediate actions both at regional and continental levels and this in line with AU Member States levels of data maturity.

References

African Development Bank. (2019). Annual Report 2019 | African Development Bank—Building today, a better Africa tomorrow. https://www.afdb.org/en/documents/annual-report-2019

Ahmed, S. (2021). A Gender perspective on the use of Artificial Intelligence in the African FinTech Ecosystem: Case studies from South Africa, Kenya, Nigeria, and Ghana. 23rd ITS Biennial Conference. https://www.econstor.eu/handle/10419/238000?author_page=1

Arntz, M., Gregory, T., & Zierahn, U. (2016). The Risk of Automation for Jobs in OECD Countries. https://www.oecd-ilibrary.org/content/paper/5jlz9h56dvq7-en

Ballell, T. R. de las H. (2019). Legal challenges of artificial intelligence: Modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review, 24(2), 302–314. https://doi.org/10.1093/ulr/unz018

Carrière-Swallow, Y., & Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective (No. 19/16). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Cavoukian, A. (2009). Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices. Information and Privacy Commissioner.

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

Couldry, N., & Mejias, U. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. SAGE Publications. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf

Deloitte. (2017). Privacy is Paramount | Personal Data Protection in Africa Personal Data Protection in Africa. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Gillwald, A., & Mothobi, O. (2019). After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Global Symposium for Regulators. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Hawthorne, S. (2020). Impact of Internet Connection on Gifted Students' Perceptions of Course Quality at an Online High School. Boise State University Theses and Dissertations. https://doi.org/10.18122/td/1748/boisestate

Information Society. (2018). Personal Data Protection Guidelines for Africa. A joint initiative of the Internet Society and the Commission of the African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

International Telecommunication Union. (2019). Measuring Digital Development Facts and

Figures (978-92-61-29511-0). https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

International Telecommunication Union. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Jones, C., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. The American Economic Review, 110(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Khan, M., & Roy, P. (2019). Digital identities: A political settlements analysis of asymmetric power and information. https://eprints.soas.ac.uk/32531/1/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

Macmillan, R. (2020). Data Governance: Towards a Policy Framework (Policy Brief No. 9). https://www.competition.org.za/ccred-blog-digital-industrial-policy/2020/7/6/data-governance-towards-a-policy-framework

Mazzucato, M., Entsminger, J., & Kattel, R. (2020). Public Value and Platform Governance (SSRN Scholarly Paper ID 3741641). Social Science Research Network. https://doi.org/10.2139/ssrn.3741641

(Mitretodis, & Euper. (2019). Interaction Between Privacy and Competition Law in a Digital Economy. Competition Chronicle. https://www.competitionchronicle.com/2019/07/interaction-between-privacy-and-competition-law-in-a-digital-economy/

Nicholas, G., & Weinberg, M. (2019). Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? | NYU School of Law. New York University School of Law. https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

OECD. (2019). Data governance in the public sector. 23–57. https://doi.org/10.1787/9cada708-en

Open Data Charter. (2015). Open Data Charter Principles. Open Data Charter. https://opendatacharter.net/principles/

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.902.7318&rep=rep1&type=pdf#:~:text=Weak%20data%20sovereignty%20as%20defined,on%20safeguard%2D%20ing%20national%20security.

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society. Research ICT Africa. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Rinehart, W. (2020, September 14). Is data nonrivalrous? Medium. https://medium.com/cgo-benchmark/is-data-nonrivalrous-f1c8e720820b

Saint, M., & Garba, A. (2016). Technology and Policy for the Internet of Things in Africa (SSRN Scholarly Paper ID 2757220). Social Science Research Network. https://doi.org/10.2139/ssrn.2757220

Savona, M. (2019). The Value of Data: Towards a Framework to Redistribute It (SSRN Scholarly Paper ID 3476668). Social Science Research Network. https://doi.org/10.2139/ssrn.3476668

Schmidt, C. O., Struckmann, S., Enzenbach, C., Reineke, A., Stausberg, J., Damerow, S., Huebner, M., Schmidt, B., Sauerbrei, W., & Richter, A. (2021). Facilitating harmonized data quality assessments. A data quality framework for observational

health research data collections with software implementations in R. BMC Medical Research Methodology, 21(1), 63. https://doi.org/10.1186/s12874-021-01252-7

Sen, A. (2001). Development As Freedom. OUP Oxford; eBook Collection (EBSCOhost). http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2089308&site=ehost-live

Stork, C., & Gillwald, A. (2012). South Africa's mobile termination rate debate: What the evidence tells us (Policy Brief No. 2; South Africa). Research ICT Africa. https://researchictafrica.net/publications/Country_Specific_Policy_Briefs/South_Africa_Mobile_Termination_Rate_Debate_-_What_the_Evidence_Tells_Us.pdf

Teh, H., Kempa-Liehr, A., & Wang, K. (2020). Sensor data quality: A systematic review. Journal of Big Data, 7. https://doi.org/10.1186/s40537-020-0285-1

UNCTAD. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow [United Nations publication].

United Nations. (2017). Looking to future, UN to consider how artificial intelligence could help achieve economic growth and reduce inequalities—United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/

van der Spuy, A. (2021, February 23). How do we protect children's rights in a digital environment only available to some? African Post. https://researchictafrica.net/2021/02/23/how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/

Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic Literature Review on the Spread of Health-related Misinformation on Social Media. Social Science & Medicine, 240, 112552. https://doi.org/10.1016/j.socscimed.2019.112552

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop, N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5

World Bank. (2021). Data for Better Lives. World Bank. Doi : 10.1596/978-1-4648-1600-0

World Bank, & ITU. (2020). The World Bank and International Telecommunication Union launch handbook on digital regulation [Text/HTML]. World Bank. https://www.worldbank.org/en/news/feature/2020/09/08/the-world-bank-and-international-telecommunication-union-launch-handbook-on-digital-regulation

World Economic Forum. (2016). Networked Readiness Index. Global Information Technology Report 2016. http://wef.ch/29cCKbU

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Penguin Publishing Group. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf

Annex - Working Definitions

Anonymisation is the removal of direct and indirect personal identifiers from data.

Continental for the purposes of this framework refers to Africa

Data classification is broadly defined as the process of organising data by relevant categories so that it may be used and protected more efficiently.

Foundational data infrastructure refers to advanced technologies which facilitate the intensive use of quality data. This may include broadband networks, data centres and cloud services, electronic hardware and software, and digital applications that are available on the Internet.

Data ecosystem- for the purposes used here not only to the programming languages, packages, algorithms, cloud-computing services, and general infrastructure an organization uses to collect, store, analyse, and leverage data, but to the underlying value chain associated with data as a factor of production, , the governance of data systems and the protection of data subjects.
Data minimisation is a principle within data protection frameworks, which entrenches collecting the minimum amount of personal data that is needed to deliver an individual element of a service or product.
Datafication refers to the process by which daily interactions of living things can be rendered into a data format and put to social and economic use.
E-commerce can be summarised as commercial transactions occurring through electronic channels - buying and selling of goods or services via the Internet, and the transfer of money and data to complete the sales - by methods specifically designed for the purpose of receiving or placing of orders.
Cloud services are used on demand at any time, through any access network, using any connected devices that use cloud computing technologies, they utilise software and applications that are located on the cloud and not on users' own devices.
Cloud-based services include mass market applications (i.e. social media and webmail offered over the Internet), whereby the data does not sit on the individuals' devices but is stored remotely in a data centre. Examples include Facebook, YouTube and Gmail.
Digital identity is a set of electronically captured and stored attributes and/or credentials that uniquely identify a person enabling the distinction of one individual from another.
Digital capability is the term used to describe the skills, literacy, social norms, and attitudes that individuals and organisations need to thrive, to live, learn and work in a digital society and economy.
Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Cybercrime: unlawful acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure (Malabo Convention)
Cybersecurity: Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. (https://digitalguardian.com/blog/what-cyber-security)
Data controller means any natural or legal person, public or private, any other organisation or association which alone or jointly with others, decides to collect and process personal data and determines the purposes.
Data protection regulates how data is used or processed and by whom, and it ensures citizens have rights over their data. It is particularly important in ensuring digital dignity, as it can directly address the inherent power imbalance between 'data subjects' and the institutions or people who collected data.

Data protection authorities (DPAs) are independent public authorities that monitor and supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints that may have breached the law.

Data subjects means any natural person that is the subject of personal data processing. (Malabo Convention)

Harmonisation is ensuring uniformity in the systems through the use of minimum standards to facilitate interoperability and legal and trust frameworks (e.g. for levels of assurance) to set rules and build confidence in respective systems.

Interoperability is the ability of different function units – e.g. systems, databases, devices, or applications – to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units (adapted from ISO/IEC 2382:2015).

Level of assurance (LOA) is the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity (ID4D Public-Private Cooperation). The overall level of assurance is a function of the degree of confidence that the applicant's claimed identity is their real identity (the identity assurance level or IAL), the strength of the authentication process (authentication assurance level or AAL), and—if using a federated identity—the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (adapted from NIST 800-63:2017).

Open standards are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (adopted from ITU-T).

Open data: Open means anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness. (http://opendefinition.org/)

(It would go just before open standards in the Working Definition annex.)

Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Privacy and security by design means proactively embedding privacy and security mechanisms into the design and operation of products and services both non-IT and IT systems, networked infrastructure, and business practices. This requires that privacy and security governance is considered throughout the whole engineering process and product lifecycle.

Pseudonymisation is the processing data in a manner so that it cannot be associated with an individual without additional information.

Regional for the purposes of this Framework refers to the five regions of Africa recognised by the African Union.

Sensitive data means all personal information relating to religious, philosophical, political opinion as well as to sex life, race, and health, social conditions of data subject (Malabo Convention)

2022-01-20

Report of the 4th Ordinary Session of the STC on Communication and ICT (STC-CICT), 25-27 October 2021

African Union

DCMP