

EAST AFRICA DATA GOVERNANCE CONFERENCE 2026



REPORT

2ND EAST AFRICA DATA GOVERNANCE CONFERENCE

THEME: NAVIGATING THE DUALITY IN DATA GOVERNANCE:
INNOVATION AND ACCOUNTABILITY IN EAST AFRICA

MARCH 10TH - MARCH 11TH 2026



Executive Summary

The 2nd East Africa Data Governance Conference 2026 was convened by the Open Institute in collaboration with Amnesty International. The meeting brought together over 150 participants drawn from 5 countries comprising policymakers, regulators, civil society organizations, private sector actors, technologists, and academics to examine the rapidly evolving landscape of data governance in the region. The conference took place at a time when East Africa is undergoing profound digital transformation. Governments are increasingly adopting digital public infrastructure, private sector organizations are leveraging data-driven technologies to innovate new services, and emerging technologies such as artificial intelligence are beginning to influence decision-making across both public and private sectors. While these developments offer unprecedented opportunities for economic growth, improved public service delivery, and regional integration, they also present complex governance challenges. Issues related to privacy protection, algorithmic accountability, cross-border data flows, and digital inequality are becoming increasingly prominent as the region's digital ecosystems expand. Against this backdrop, the conference created a platform for regional dialogue on how East African countries can harness the benefits of digital innovation while safeguarding human rights, accountability, and public trust.

The 2026 conference was organized under the theme "Navigating Duality in Data Governance." The theme reflected a central tension shaping contemporary digital governance debates: the perception that innovation and accountability are competing priorities. Discussions throughout the conference challenged this assumption, emphasizing that sustainable digital development requires governance frameworks that allow innovation to flourish while ensuring that technological systems operate within clear ethical, legal, and human rights boundaries. Participants engaged in a series of plenary discussions, panel sessions, lightning talks, and breakout dialogues exploring key dimensions of data governance in the region. These discussions were organized around five thematic pillars: data ownership and custodianship; sovereignty and cross-border governance; infrastructure, interoperability, and standards; ethics, algorithms, and accountability; and the economics and value of data. Together, these pillars provided a framework for examining the political, economic, and social implications of data-driven systems in East Africa.

Several key insights emerged from the conference discussions. Participants emphasized that while many countries in the region had already established legal frameworks for data protection and digital governance, implementation remains a significant challenge. Bridging the gap between policy commitments and practical enforcement will require stronger institutional capacity, greater regulatory clarity, and sustained investment in public awareness and digital literacy. Another emerging issue was the importance of regional collaboration in addressing the challenges of cross-border data governance. As digital systems increasingly transcend national boundaries, isolated national approaches to regulation were becoming less effective. Participants highlighted the need for harmonized regulatory frameworks that can facilitate trusted cross-border data flows while protecting citizens' rights.

The conference also underscored the need for human-centered approaches to data governance. Speakers repeatedly stressed that technological innovation must not come at the expense of dignity, privacy, or equality. Instead, governance frameworks must ensure that individuals and communities remain at the center of digital transformation processes. In addition, discussions highlighted the importance of digital inclusion and capacity building, particularly for marginalized communities such as women, youth, and rural populations. Without deliberate efforts to expand digital skills and access, there is a risk that the benefits of the data economy will remain concentrated among a small segment of society.

Overall, the conference reaffirmed the importance of continued regional dialogue and multi-stakeholder collaboration in shaping the future of digital governance in East Africa. Participants emphasized that building trusted digital ecosystems will require cooperation between governments, private sector actors, civil society organizations, and academic institutions.

Ultimately, the conference addressed the overarching question of how can East Africa advance digital innovation while safeguarding rights, trust, and accountability in governance as captured in this detailed report.

+150

ATTENDEES

+5

COUNTRIES REPRESENTED

+2500

ONLINE VIEWERS



Innovation grows where trust is built. Data protection is not a barrier to innovation, it is the foundation that allows people and institutions to trust digital systems

Immaculate Kassait

Office of the Data Protection
Commissioner, Kenya



Conference Background

Over the past decade, East Africa has experienced rapid expansion in the adoption of digital technologies across both public and private sectors. Governments are increasingly investing in digital public infrastructure to improve service delivery, expand financial inclusion, and strengthen administrative efficiency. Digital platforms are now widely used in sectors such as healthcare, agriculture, education, and financial services, while innovations in fintech, mobile money, and data analytics have positioned the region as one of Africa's most dynamic digital ecosystems. At the center of this transformation lies data. Data increasingly informs public policy decisions, powers digital services, supports innovation, and drives economic activity. However, as the collection and use of data expands, so too do the governance challenges associated with managing it responsibly. Questions around privacy, digital surveillance, algorithmic bias, cross-border data flows, and unequal access to digital opportunities are becoming increasingly prominent in policy and governance discussions across the region.

In response, many countries in East Africa have begun to establish legal and institutional frameworks to regulate the use of personal data and strengthen digital governance. Kenya, Uganda, and Tanzania have enacted data protection laws and established regulatory authorities responsible for overseeing compliance and protecting citizens' rights in digital environments. Regional and continental frameworks, including those developed by the African Union, have also sought to guide the development of harmonized data governance approaches across Africa. Despite these efforts, the practical implementation of data governance frameworks continues to present challenges. Regulatory institutions often face capacity constraints, public awareness of data rights remains limited, and the rapid emergence of new technologies such as artificial intelligence is introducing governance questions that existing frameworks are still adapting to address. At the same time, the increasingly transnational nature of digital systems means that questions of data governance cannot be effectively addressed within national boundaries alone.

It is within this evolving landscape that the 2nd East Africa Data Governance Conference was established as a regional platform for dialogue and collaboration. The conference brings together policymakers, regulators, technologists, academics, civil society leaders, journalists, and development partners to collectively reflect on the challenges and opportunities shaping the region's digital future. By creating a space for exchange across sectors and countries, the conference seeks to contribute to the development of governance frameworks that are both responsive to technological change and grounded in principles of accountability, inclusion, and human rights. The 2026 edition of the conference was organized under the theme "Navigating Duality in Data Governance." The theme reflects a growing recognition that innovation and accountability are often framed as competing priorities in debates about digital governance. In practice, however, sustainable digital transformation requires that these two imperatives evolve together. Technological systems that prioritize innovation without adequate safeguards risk undermining public trust and exacerbating social inequalities, while overly restrictive regulatory environments can slow innovation and limit opportunities for economic growth.

The concept of duality therefore captures the central tension shaping East Africa's current digital moment. Across the region, governments and institutions are building new systems of data-driven governance while simultaneously grappling with heightened concerns about privacy, surveillance, the concentration of power in digital platforms, and the potential exclusion of marginalized communities from the benefits of the digital economy. Addressing these challenges requires governance approaches that enable innovation while safeguarding justice, rights, and public trust. To guide the conversations, the conference was structured around five interrelated thematic pillars reflecting key dimensions of contemporary data governance debates.

Key Conference Pillars



At the Open Institute, we are particularly concerned about the number of people who may be left behind due to a lack of data-related skills, and the urgent need to equip communities with the knowledge and tools to meaningfully participate in the data-driven world

Al Kags
Founder and Executive Director-Open
Institute

05.

Fifth pillar examined the economics and value of data, exploring the political economy of digital systems. As data becomes an increasingly valuable asset in global digital economies, questions arise about how that value is generated, who benefits from it, and what governance models can ensure that citizens and public institutions share in the returns generated from data-driven innovation.

01.

One area of focus concerned data ownership and custodianship, exploring fundamental questions about who holds rights over citizen-generated data and how responsibility for safeguarding that data should be shared among governments, corporations, digital platforms, and public institutions. As data increasingly becomes both a governance resource and an economic asset, debates around ownership, control, and stewardship are becoming central to discussions about digital rights and accountability.

02.

Second pillar examined sovereignty and cross-border data governance, recognizing that digital systems increasingly transcend national borders. As data flows move across jurisdictions, East African countries must navigate complex questions about how to assert control over national data ecosystems while supporting regional integration and cross-border digital services.

03.

Third pillar explored infrastructure, interoperability, and standards, focusing on the foundational systems that enable trustworthy digital governance. Discussions under this pillar highlighted the importance of designing digital infrastructures that are secure, interoperable, and capable of supporting trusted data exchange across institutions and sectors.

04.

Fourth pillar addressed ethics, algorithms, and accountability, examining the growing influence of artificial intelligence and automated decision-making systems in both public administration and private sector operations. As algorithms increasingly shape decisions affecting access to services, financial inclusion, and public resources, ensuring fairness, transparency, and accountability in these systems has become a critical governance challenge.

Day 1

Conference opening and Keynote address

The conference opened with welcoming remarks delivered by Christine Ajulu from the Open Institute on behalf of the organizing partners noting the regional character of the conference and the importance of cross-border collaboration in addressing data governance challenges. Participants were encouraged to use the conference as an opportunity not only for learning but also for building partnerships that could extend beyond the two-day event.



Context Setting

In his introductory remarks, Mr. Philip Kisaka, the master of ceremony reflected on the broader regional context within which the conference was taking place. He noted that the East African region is currently experiencing a period of significant transition driven largely by technological change and the rapid expansion of digital systems. Governments are increasingly investing in digital platforms to deliver public services, private companies are leveraging data analytics to innovate new products, and artificial intelligence is beginning to influence decision-making processes across multiple sectors. However, he cautioned that the rapid pace of technological development had not always been matched by equally robust governance frameworks. As a result, policymakers and practitioners were grappling with complex questions about how to regulate digital systems without stifling innovation. He emphasized that conversations about cross-border data flows, digital identity systems, and the regulation of emerging technologies are becoming increasingly prominent across the region. These issues underscored the importance of spaces such as the East Africa Data Governance Conference, where diverse stakeholders can come together to deliberate on the future of digital governance. He recognized the presence of the Director General of the Personal Data Protection Commission of Tanzania and other high-level regulatory officials, noting that their participation reflected growing government engagement in regional data governance discussions.

The Opening remarks were delivered by Victor Ndede, Head of Programs at Amnesty International Kenya, who was standing in for Amnesty International's Executive Director, Irungu Houghton. Ndede welcomed participants to the conference and emphasized the importance of building sustained dialogue around data governance issues in the region. He explained that the conference was established as a platform where stakeholders could collectively reflect on the challenges and opportunities emerging from the digital transformation taking place across East Africa.



He noted that the region was at a critical juncture where decisions about how data is governed would have long-term implications for economic development, democratic governance, and the protection of human rights. As governments increasingly adopt digital technologies to manage public services and economic activities, it becomes essential to ensure that appropriate safeguards are in place to protect individuals from harm. He expressed hope that the conference would provide a conducive space for participants to exchange ideas, learn from each other's experiences, and identify practical strategies for strengthening data governance frameworks in East Africa.

Reflections from the Open Institute

By Al Kags, Founder and Executive Director

In his opening remarks, Al Kags, Founder and Executive Director of the Open Institute, reflected on the growing importance of data governance conversations across the continent. He observed that data played a central role in shaping economic, political, and social systems. Governments, corporations, and development organizations are increasingly relying on data to inform decision-making and drive innovation. Despite the growing availability of policies and regulatory frameworks addressing data governance across East Africa, Kags emphasized that implementation remains a major challenge.



Many countries have adopted legislation related to data protection and digital governance, but translating these frameworks into everyday practice remains difficult. He highlighted the importance of bridging the gap between policy and practice, noting that discussions about data governance must extend beyond legal frameworks to include the practical realities of how data is collected, processed, and used by institutions. Al Kags also drew attention to the issue of public awareness referencing a recent campaign conducted through the Mudata initiative, in which a healthcare worker was recorded publicly disclosing a patient's medical condition while calling out names in a waiting area. The incident sparked widespread discussion about privacy and the handling of personal data in everyday contexts. The example illustrated that while policies may exist, many individuals and institutions still lack a clear understanding of their responsibilities in handling sensitive data. Al Kags emphasized that addressing this gap will require significant investments in public awareness and digital literacy. He then welcomed Mr. Davis Adieno, the board chair of open institute to give his opening remarks.

Davis Adieno, Board Chair of the Open Institute

Following the remarks by Al Kags, Davis Adieno, Board Chair of the Open Institute and Chief Operating Officer of lamtheCODE, welcomed participants to the conference on behalf of the organization's board. In his remarks, he acknowledged the growing significance of the East Africa Data Governance Conference as a platform for critical dialogue on the region's digital future. He highlighted the work of lamtheCODE, describing it as an African-led global movement that seeks to equip young people, particularly girls and women with skills in STEM education, digital literacy, and artificial intelligence. Through partnerships and coalition building, the initiative aimed to accelerate the development of digital skills that will enable African youth to actively participate in shaping the technologies and economies of the future.



Reflecting on the origins of the conference, Adieno noted that the East Africa Data Governance Conference began as a modest experiment intended to explore emerging issues related to artificial intelligence and other rapidly evolving technologies. Over time, however, the convening has grown into a significant regional forum that brings together policymakers, technologists, researchers, civil society actors, and private sector stakeholders to engage with the broader implications of digital transformation.

He emphasized that alongside the opportunities presented by technological innovation, there remain legitimate and pressing concerns related to privacy, the ethical use of data, and the governance of digital systems. Adieno further stressed that conversations about data governance must remain grounded in the lived experiences of citizens. As data increasingly shapes decision-making across sectors, it becomes essential to ensure that citizens have a voice in how data is produced, managed, and applied. He ended by saying that the conference continues to play an important role in amplifying these perspectives while fostering dialogue on responsible and inclusive approaches to data governance in the region.

Remarks by Lady Marième Jamme, Founder- lamthe CODE



Powerful remarks were made by Lady Marième Jamme, Founder of the global movement lamtheCODE. Speaking from her extensive experience in promoting digital literacy and coding education among women and girls, she emphasized the fact that data was rapidly becoming one of the most valuable resources in the digital economy and warned that the benefits of this new data-driven economy were not being distributed equally. She added that women, young people, and marginalized communities often lacked access to the digital skills needed to participate meaningfully in the digital ecosystem.

Drawing on examples from refugee communities such as Kakuma and Dadaab in Kenya, Lady Marième Jamme highlighted the creativity and resilience of women and girls who are teaching themselves coding and building digital tools despite limited access to resources. These examples, she argued, demonstrated the immense potential that existed within marginalized communities when individuals are given the opportunity to develop digital skills. She emphasized that the ability to understand and work with data was becoming a fundamental skill in the modern world. Teaching communities how to collect, analyze, visualize, and interpret data was therefore essential for ensuring that they are not left behind in the digital economy.

Remarks by Dr. Mugambi Laibuta - Chairperson, Data Privacy and Governance Society of Kenya

Dr. Mugambi Laibuta, Chairperson of the Data Privacy and Governance Society of Kenya, addressed participants by emphasizing the importance of professional collaboration and capacity building within the rapidly evolving field of data governance. He welcomed conference participants and encouraged practitioners, regulators, researchers, and students to consider engaging with the Society as a platform for professional development and knowledge exchange. Dr. Maguta highlighted that one of the most pressing challenges facing the data governance ecosystem in the region was the shortage of skilled professionals with interdisciplinary expertise. Data governance, he noted, is inherently complex and cannot be effectively addressed through a single disciplinary lens. Instead, it requires collaboration among diverse professionals including technologists, lawyers, policy experts, researchers, students, and private sector actors. He added that the Society brought together individuals from a wide range of backgrounds including legal professionals, data scientists, academics, and industry practitioners to foster dialogue and shared learning within the field. He stressed that discussions on data governance cannot take place in institutional or disciplinary silos and required coordinated engagement between practitioners who design and implement digital systems and regulators who are responsible for ensuring that those systems operate within legal and ethical frameworks. Without such collaboration, significant gaps can emerge between policy development and practical implementation.

Dr. Laibuta also emphasized the importance of nurturing the next generation of data governance professionals. As part of its efforts to encourage critical thinking and innovation among young scholars, the Society recently organized an essay competition focused on the theme of surveillance and data governance. The competition attracted submissions from students exploring complex issues surrounding data rights, privacy, and governance in contemporary digital environments.



One of the winning essays examined the implications of data surveillance within refugee contexts, highlighting the vulnerabilities that displaced populations may face within digital systems. He underscored that providing platforms for mentorship and intellectual exchange is essential for building a robust ecosystem of practitioners capable of addressing the evolving challenges posed by digital technologies. By supporting such initiatives, the Society sought to create opportunities for mentorship and learning for emerging professionals who are interested in contributing to the development of responsible data governance frameworks. In closing, he encouraged stakeholders across the region to embrace a strong spirit of collaboration. Effective data governance, he noted, depended on continuous engagement between regulators, practitioners, civil society actors, and the private sector. When these actors work together, it becomes possible to develop governance systems that both enable innovation and protect the rights and dignity of individuals in an increasingly data-driven world.

Opening Remarks from Regional Data Protection Leaders

Remarks by Edna Kasozi- Personal Data Protection Office in Uganda



Ms. Edna Kasozi from the Personal Data Protection Office in Uganda welcomed heads of data protection authorities, policymakers, researchers, civil society actors, and private sector representatives who had convened for the conference. She expressed appreciation to the organizers for creating a platform that brought together regulators, policy makers, and thought leaders from across the region to deliberate on emerging governance challenges in the digital age. In her remarks, Kasozi noted that the conference theme, “Value and Vulnerability of Digital Public Infrastructure,” spoke directly to

one of the defining policy questions of the present moment. She observed that digital technologies were rapidly transforming multiple sectors across East African economies, including public administration, healthcare, agriculture, education, financial services, and urban development initiatives such as smart cities. She underscored the fact that data now underpinned nearly every sector of modern economies, fueling innovation, improving service delivery, and enabling new models of governance and economic participation. Drawing from Uganda’s national experience, she highlighted how investments in digital public infrastructure have already begun to reshape service delivery in the country.

Key initiatives such as the national identification system administered by the National Identification and Registration Authority, the expansion of the national digital payments ecosystem, and integrated government service platforms illustrate how digital infrastructure can expand financial inclusion and improve administrative efficiency. These initiatives demonstrate the transformative potential of digital systems when effectively implemented. Ms. Kasozi emphasized that such transformation must be guided by strong governance frameworks.

Data protection and digital governance, she argued, must never be treated as an afterthought, instead, privacy and data protection considerations must be embedded into digital systems from the earliest stages of design and implementation. The central challenge facing regulators was therefore striking a deliberate balance between enabling the productive use of data while simultaneously protecting individuals from harm. She further explained that Uganda's Personal Data Protection Office was working to operationalize the country's data protection framework through several key strategies including expanding public awareness on data rights, strengthening institutional systems for data protection oversight, and fostering collaboration between government institutions, private sector actors, and civil society organizations. Encouragingly, she noted that awareness among citizens regarding their data rights is steadily growing, reflecting increasing public engagement with digital governance issues. Kasozi also stressed that no country can effectively govern data in isolation. In a digitally interconnected world, data flowed seamlessly across national borders, making regional dialogue and cooperation essential. Strengthening regional cooperation among East African countries facilitated trusted cross-border data flows, strengthened collective cybersecurity resilience, improved enforcement coordination among regulators, and provided greater regulatory certainty for businesses and innovators operating across multiple jurisdictions.

At the same time, she cautioned that regional harmonization efforts must not dilute the fundamental protections afforded to citizens. Individuals must remain at the center of all digital governance interventions, with frameworks anchored in principles such as transparency, accountability, fairness, and proportionality. She challenged participants to reflect on fundamental questions that shaped the region's digital future: who ultimately controls data; who bears responsibility when data misuse causes harm; and how governments can balance the efficiencies offered by digital systems with the protection of individual rights. Ms. Kasozi concluded by emphasizing the importance of strengthening regulatory capacity, promoting policy coherence across institutions, and investing in collaboration mechanisms that support responsible innovation. She underscored that data governance must contribute to inclusive development, ensuring that digital transformation does not deepen existing inequalities or exclude vulnerable groups. Particular attention, she noted, must be given to ensuring that women, marginalized communities, and other vulnerable populations are not left behind in the digital transition. She reaffirmed Uganda's commitment to working with neighbouring countries to strengthen regional cooperation and advance responsible digital infrastructure across East Africa.

Dr. Emmanuel Mkilia (Dr. Kaliya) - Personal Data Protection Commission, Tanzania

Dr. Emmanuel Mkilia, Director at the Personal Data Protection Commission in Tanzania, shared reflections from Tanzania's experience in establishing and strengthening its national data protection framework. He noted that this was his first time attending the East Africa Data Governance Conference and expressed appreciation for the opportunity to engage with peers from across the region. Dr. Mkilia explained that his appointment as Director General of Tanzania's data protection authority coincided with a period of rapid institutional development. Shortly after assuming office, he embarked on a regional learning visit, including engagements with counterparts in Kenya to understand

approaches to operationalizing data protection frameworks. These early consultations informed the development of a focused 100-day institutional plan aimed at strengthening the operational foundation of Tanzania's data protection authority. The plan prioritized four key areas: raising public awareness about data protection, strengthening compliance among institutions that process personal data, building internal capacity within the regulatory authority, and establishing effective enforcement mechanisms. These pillars, he noted, were essential for building a credible and effective regulatory environment capable of responding to emerging digital governance challenges.



Dr. Mkilia framed the conference discussions around what he described as two critical dimensions of technological development. The first dimension related to technological advancement itself, the innovation, creativity, and experimentation that drove digital transformation. The second dimension, which he emphasized as equally important, was the human dimension. At its core, digital transformation must ultimately serve people and improved service delivery without compromising the dignity and rights of individuals whose data formed the foundation of digital systems. He stressed that while technological innovation continued to advance rapidly, the individuals whose data fuelled these systems must never be reduced to mere components within digital ecosystems. Instead, they must remain at the center of governance frameworks that safeguard their rights, dignity and agency.

Dr. Mkilia also explained that in Tanzania, data protection considerations were increasingly being integrated across the broader technology ecosystem. Institutions responsible for technological innovation including startups, developers, and digital service providers were expected to integrate privacy and security considerations from the design stage. Embedding these principles within innovation processes not only protects citizens but also strengthen trust in the digital economy, which in turn supports broader economic development.

Immaculate Kassait - Data Protection Commissioner, Kenya

Ms. Immaculate Kassait, Data Commissioner of Kenya's Office of the Data Protection Commissioner, delivered remarks highlighting the importance of regional collaboration in shaping the digital future of East Africa. She noted that it was a privilege to join stakeholders from across the region to reflect collectively on the governance challenges and opportunities emerging from rapid technological transformation. Kassait emphasized that digitization was no longer optional in either the public or private sector. Digital technologies have become essential tools for improving service delivery, driving innovation, and enabling economic growth.



As governments and businesses increasingly rely on digital platforms and data-driven systems, however, it was critical to ensure that these technologies operate within strong governance frameworks. She noted that the challenges posed by emerging technologies required a multisectoral response involving governments, regulators, private sector innovators, academia, and civil society organizations. Balancing technological advancement with the principles of good governance required coordinated efforts across institutions and sectors.

Ms. Kassait also highlighted the broader continental direction set by the African Union in strengthening digital governance frameworks. In particular, she referenced the African Union Data Policy Framework, which provided strategic guidance for African countries on managing data in ways that promoted innovation while safeguarding citizens' rights. The framework emphasized the need for ethical data management systems, strengthened data protection institutions, and greater harmonization of data governance practices across the continent. She further noted that globally, more than 170 countries had established legal frameworks for data protection, demonstrating the increasing recognition of the importance of safeguarding personal data in the digital age. Rather than viewing data protection as a barrier to innovation, Kassait emphasized that strong data governance frameworks actually enabled innovation by fostering trust within digital ecosystems.

Kassait also highlighted the practical regulatory challenges faced by businesses operating across multiple jurisdictions in East Africa. Differences in national legal frameworks and regulatory requirements can create compliance challenges for investors and technology companies seeking to operate regionally. Harmonizing technology-related policies, particularly those related to data protection, would therefore help reduce regulatory uncertainty and made the region more attractive for innovation and investment. To address some of these challenges, Kenya's Office of the Data Protection Commissioner had developed guidance documents that clarified the roles and responsibilities of data controllers and data processors.

These resources aimed to reduce uncertainty for organizations operating within Kenya and across borders while strengthening compliance with national data protection regulations. She also emphasized the importance of strengthening enforcement collaboration among regulators in the region. Coordinated enforcement mechanisms, she argued, would send a stronger message regarding the seriousness with which East African countries approached data protection obligations.

Ms. Kassait encouraged conference organizers to consider rotating the location of the conference across different countries in the region, such as Uganda and Tanzania, to further strengthen regional ownership of the dialogue. She also urged practitioners and policymakers to carefully consider the types of digital systems being adopted across the region, noting that the governance choices made today would shape the long-term digital landscape of East Africa. In conclusion, she reflected on emerging global conversations around the economic value of personal data, referencing emerging models in countries such as Brazil where individuals may be compensated for the use of their personal data. Kassait noted that such developments signal a shift in the global conversation from traditional competition law debates about monopolies toward broader discussions on data ownership, value distribution, and digital economic rights.

PANEL DISCUSSIONS

Plenary Panel 1: Governing in the Grey - Can East Africa Balance Tech Growth with Rights?

Panelists: Florence Syevuo (SDG Kenya forum), Rosemary Koech (KCB), Diana Gichengo (Director TISA Kenya), Dr. Mugambi Laibuta (DPGSK), Dr. Emmanuel Mkilia (DG Data protection commission of Tanzania), Ms. Immaculate Kassait (Office of Data protection commission Kenya)



The first panel explored the complex intersection of technological innovation and the protection of fundamental rights. Moderated by Victor Ndede, it brought together representatives from government, civil society and the legal profession to reflect on governance challenges arising from rapid technological change. Panelists highlighted the increasingly blurred boundaries between innovation and regulation. While digital technologies offered significant potential for economic growth and improved public services, they also introduce risks related to surveillance, data misuse and erosion of privacy. Rosemary Koech, an advocate of the high court of Kenya and Data Protection Officer at KCB group, emphasized that communities must be actively engaged in shaping how technologies are deployed. She cautioned against assuming that communities will naturally adapt to new technologies without participation in decision-making processes. A major focus of the discussion was the evolving concept of digital identity. Beyond traditional documents like passports or national identity cards, digital identities were now constructed from online interactions, social media activity, financial transactions, and other digital footprints. This shift raised critical governance questions about individual control over personal data and how institutions should regulate its use in decision-making.

Panelists stressed that digital governance was a shared responsibility. Regulators, private sector innovators, civil society organizations, and citizens each played distinct but interconnected roles in shaping how data systems operated. The multi-stakeholder approach was emphasized as essential, as isolated institutional efforts were insufficient to address the complexities of data governance. Trust in digital systems emerged as another key theme. Private sector participants highlighted that trust was foundational for sectors handling sensitive personal data, including finance, telecommunications, and healthcare. They described governance measures such as employee training, internal compliance frameworks, and accountability mechanisms to safeguard personal information. The panel acknowledged the role of academia and research institutions in informing data governance frameworks. They noted that universities provided evidence-based insights and neutral platforms for analysis and guidance on societal implications of emerging technologies, supporting governments and regulators in developing informed policies. These discussions set the stage for subsequent breakout sessions, where participants engaged in focused dialogue on specific thematic areas.



FROM LEFT: Florence Syevuo (SDG Kenya forum), Rosemary Koech (KCB), Diana Gichengo (TISA Kenya), Dr. Mugambi Laibuta (DPGSK), Dr. Emmanuel Mkilia (DG Data protection commission of Tanzania), Ms. Immaculate Kassait (Office of Data protection commission Kenya) and Victor Ndede (panel moderator)

BREAKOUT SESSION 1

Track 1: Data Ownership and Custodianship Data Sovereignty

Title: Whose Data Counts? Participation, Power and Inclusive Governance

Panelists: United Disabled Persons of Kenya (UDPK), Maono Space

Lead Organization: Global Partnership for Sustainable Development Data (GPSDD)

This session examined the question of who ultimately owns and controls data generated within East African digital ecosystems. Participants discussed the evolving concept of data sovereignty and its implications for governance, economic development, and citizen rights. Eric from United Disabled Persons of Kenya (UDPK), recognized that the efforts to collect and use data has had immense roles in championing issues with PWDs yet there were still barriers that entrench inequality which limits proper usage of data to enhance better life for PWDs. Some of the barriers that face disability data have been raised through UDPK but these have not resulted in collective action towards ensuring that PWDs are at the centre of making their data to be used in a way that benefits them. He spoke of a program known as Data value by Global Partnership for Sustainable Development Data (GPSDD) which has leveraged collective action that has championed for having a fair data future to give PWDs the power to be able to influence the data that is shaping their own lives. He noted that many times PWDs were left out in data processes in Kenya. Lydia Furaha from Maono space in Kilifi, a data value advocate portrayed advancements noting that communities were now owning the data that shapes their lives and living realities, unlike before when programs were being funded based on data that does not speak to the community real lives.

Questions posed to the audience during the discussion were:

- Who decides what is counted?: Participants noted that decisions about what data is collected and how it is measured are often made by institutions with technical capacity and resources, such as governments, technology companies, and research organizations. As a result, communities that lack representation in decision-making processes find their realities underrepresented or misrepresented in datasets. Participants emphasized that determining “what counts” should not be left solely to technical experts. Instead, data collection processes should involve community consultation and stakeholder engagement, ensuring that the priorities and lived experiences of citizens inform what information is gathered and how it is used.
- What does representation mean when data is aggregated, anonymized or automated? Participants acknowledged that while aggregation and anonymization are essential for protecting privacy, they can sometimes obscure important social differences and local realities. When data is aggregated at high levels, it may mask inequalities affecting specific groups or communities. Participants also highlighted that automated systems relying on aggregated datasets can reproduce existing biases if those datasets fail to reflect diverse populations. For example, algorithms trained on incomplete or biased datasets may generate outcomes that disadvantage certain communities.
- How can participation be built into systems rather than added as an afterthought? Several approaches were proposed to achieve meaningful participation:
 - **Co-design processes** - where communities contribute to the design of digital services and data governance frameworks.
 - **Public consultation mechanisms** - during policy development and system implementation.
 - **Feedback loops and accountability channels** - that allow citizens to challenge decisions or request corrections to data affecting them.
 - **Digital literacy initiatives** - to ensure citizens understand their rights and can meaningfully engage in governance processes.

Participants agreed that integrating participation into system design would help build trust, transparency, and legitimacy in digital governance frameworks.



From Left: Lydia Furaha-Maono Space, Eric Sande-United Disabled Persons of Kenya (UDPK)

Track 4: Ethics, Algorithms, and Accountability

Title: When Data Decides Who Gets Care?

Lead Organization: The Institute for Social Accountability (TISA)

This session, facilitated by Vyrone Otieno of TISA (The Institute for Social Accountability) Kenya, provided a critical examination of the intersection between data governance and the constitutional right to health. The presentation focused on the growing use of digital systems and data, particularly Proximal Means Testing (PMT), to determine eligibility and premiums under Kenya's new Social Health Insurance Fund (SHIF). Vyrone opened the session with a series of provocative questions designed to frame the ensuing debate. He challenged the audience to consider whether access to a fundamental right like healthcare should hinge on how a digital system classifies an individual using a limited set of data. He asked what happens when these automated systems get it wrong, questioning whether the pursuit of administrative efficiency can ever justify exclusion from essential health services or the imposition of caps on health access.



These reflections underscored a central theme: the urgent need to define and protect citizen rights over the data used to make life-altering decisions. The presentation established that Kenya's data governance debate is rooted in a fundamental tension. He noted that while on one hand, health was a constitutionally guaranteed right, placing a clear obligation on the state to ensure access without discrimination. On the other hand, this ideal was challenged by practical pressures, including significant fiscal strain from public debt and a growing population. It is within this gap between rights and resources that governments are turning to data-driven tools. Vyrone explained that governments facing fiscal pressure often responded by trying to target subsidies more narrowly, ensuring that limited public funds went primarily to those deemed most in need. Means. In the Kenyan context, this has manifested in the SHIF, during registration, individuals provided primary information online and an algorithm then used this data to generate a "welfare score," which determined both their eligibility for subsidies and the premium they must pay. As Vyrone noted, PMT was particularly attractive in environments like Kenya and the wider EAC, where formal income data is limited, as it uses proxy indicators to classify households. A significant portion of the session was dedicated to the profound accountability challenges that arose from this automated, data-dependent system. Vyrone outlined a chain of impunity where responsibility becomes diffuse:

1. For the Citizen: When an individual is denied access to healthcare due to an inability to pay a premium, because the system has classified them as able to contribute accountability becomes a major issue.
2. For the Health Facility: A citizen seeking recourse at a health facility is often told that the decision was made by "the system," leaving the facility with no power to overrule it.
3. For the Administrators: System administrators, in turn, may deflect responsibility by pointing to the data that the algorithm used to generate the premium.
4. For the Data Source: The data itself may originate from third-party records, such as M-Pesa transaction histories, over which the individual has a very limited ability to review, challenge, or correct inaccuracies.

Vyrone summarized the core risks associated with this approach, highlighting the following key concerns:

- Exclusion errors where genuinely vulnerable individuals are mistakenly deemed ineligible.
- Misclassification of vulnerability due to flawed proxy indicators that do not accurately reflect a household's economic reality.
- A complete lack of accountability regarding the premium payment decisions made by the algorithm.
- Weak or non-existent appeal mechanisms that would allow citizens to contest their classification.
- A limited public understanding of how these complex decisions are made, creating an opaque system that erodes trust.

In closing, Vyrone made a compelling case for why citizen voice is not just beneficial but essential in the governance of PMT and data used for health access. He argued that meaningful participation provided a "conversational right," connecting people to the systems that govern them by enabling them to review, question, and update their information. Citizen engagement was the primary mechanism for ensuring transparency and accountability in digital systems. Furthermore, he stressed that only through direct feedback from communities can these systems begin to meet the complex local realities of informal economies, which were often invisible in official datasets. The presentation was followed by a robust plenary discussion in which participants raised important questions on whether the current methods used to determine Social Health Authority (SHA) premium contributions truly reflected citizens' socioeconomic realities. There was a strong and collective call for the government to revisit the current approach and ensure the system was fair, transparent, and trusted by the public. Participants emphasized that building trust required meaningful community involvement, starting conversations at the lowest levels so that communities clearly understand how the system works and how contribution levels are determined. The need for a clear redress mechanism within the existing system was also highlighted, allowing citizens to effectively challenge or seek clarification on how their premiums were assessed. A key outcome of the session was the agreement that these critical discussions would inform the submission of a formal memorandum. This memorandum will capture stakeholder recommendations and serve as a consolidated voice to strengthen accountability, transparency and citizen trust in the system.



Vyrone Otiemo- TISA Kenya



Conference delegates in an ongoing breakout session by TISA Kenya

Track 5: Economics & Value of Data (Monetization & Shared Benefit)

Title: Integrating Evidence and Practice for Data Governance and Accountability in Africa

Lead Organization: Centre for the Study of the Economies of Africa (CSEA)

During this breakout session, the discussion focused on how evidence, research, and practical tools could strengthen data governance, accountability, and ethical data practices across Africa. The session featured two complementary presentations delivered by Adedeji Adeniran from the Centre for the Study of the Economies of Africa (CSEA) and Solomon Samo, a data analyst.

Together, the presentations explored the current realities of data governance in Africa, the challenges in ensuring accountability in data analysis, and practical frameworks to improve transparency and reproducibility in data-driven decision-making.

Presentation 1: AI Usage and Data Governance in Digitally Enabled Firms by Adedeji Adeniran (CSEA)

Adedeji Adeniran's presentation focused on the growing use of artificial intelligence (AI) in African businesses, particularly in Nigeria, and its implications for data governance, ethics, and economic development. The study aimed to generate empirical evidence on how firms are adopting AI technologies and the governance challenges associated with this adoption. He pointed out that the study was motivated by the recognition that while AI was increasingly transforming industries globally by improving efficiency and reducing costs, the benefits remained unevenly distributed. There was a real concern that developing countries could receive only a small share of the global gains from AI unless proactive policy and governance measure were put in place. Despite growing interest in these technologies across the continent, localized evidence on how businesses were actually using AI tools, the risks they encounter, and the governance structures guiding their deployment remained limited. To address this evidence gap, the study employed a firm-level survey of 530 digitally enabled businesses in Nigeria.

A structured questionnaire was administered electronically to collect comprehensive information on AI adoption trends, the drivers and barriers to adoption, the economic benefits realized, the risks and vulnerabilities encountered, and the ethical concerns and data governance practices within these firms. The survey captured a wide range of business sizes, from micro enterprises with fewer than ten employees to large firms with more than two hundred employees, ensuring a representative view of the business landscape. The findings revealed that AI adoption was indeed increasing across businesses, but the pattern of adoption is uneven. Larger firms emerged as the earliest adopters, with many reporting usage of AI tools for more than five years. In contrast, micro and small enterprises were largely late adopters, highlighting significant disparities in technological capacity and access to resources.



Despite these differences, many businesses across all categories reported moderate to high levels of AI usage, suggesting that AI was becoming integrated into everyday business operations rather than remaining an experimental tool. The benefits reported by firms using AI were substantial leading to improved operational efficiency, reduced costs, enhanced service delivery, and expanded market reach. However, alongside these benefits, the study also identified several prominent risks and concerns including high economic cost of implementing and maintaining AI systems, data security risks, data privacy concerns, and the accuracy and reliability of AI-generated data. Interestingly, concerns about job displacement and regulatory compliance were relatively low among the surveyed firms. From an ethical perspective, firms expressed significant concern about safety and cybersecurity risks, data privacy, transparency in AI decision-making, and the level of digital literacy among users. Issues such as fairness and non-discrimination, however, were reported as relatively lower priorities across many firm categories. In response to these risks, businesses were adopting several mitigation strategies, with employee training on ethical AI use emerging as the most common and cost-effective approach. Other proposed strategies include the implementation of internal ethical guidelines, enhanced cybersecurity systems, and the conduct of regular audits.

Policy Recommendations

To address existing gaps and maximize the benefits of AI, the presentation proposed several recommendations:

1. Governments should introduce financial incentives such as AI innovation grants and tax incentives to reduce implementation costs, especially for small businesses.
2. Firms should invest in continuous workforce training and upskilling to address talent shortages.
3. Policymakers should establish clear AI governance frameworks and ethical guidelines to reduce regulatory uncertainty.
4. Governments should create state-led systems for monitoring AI risks and breaches to ensure responsible deployment of AI technologies.

Presentation 2: Closing the Data Accountability Gap in Africa by Solomon Samo

The second presentation, delivered by Solomon Samo, built upon the empirical findings by shifting focus to a critical and often overlooked challenge in data governance: the lack of transparency and reproducibility in data analysis processes. Samo examined what he termed the "analytical accountability gap," a phenomenon where policy decisions and public reports rely on data analysis that is not transparent, reproducible, or verifiable. He argued that trust in data-driven policymaking is fundamentally dependent on transparency in how data is analyzed. When analytical processes remain hidden or undocumented, the evidence produced becomes difficult, if not impossible, to verify. This creates what is often described as an "analysis black box," where stakeholders are unable to understand or reproduce the steps taken to arrive at a given conclusion. Without the ability to reproduce results, Samo cautioned, analysis risks becoming little more than opinion dressed up as evidence. To illustrate the real-world consequences of such opaque analytical practices, the presentation drew on several regional case studies



from East Africa. In Kenya, a report examining public awareness of the Data Protection Act revealed that awareness of data rights remained low to moderate, particularly among rural and marginalized communities. This gap was compounded by weak enforcement capacity and the limited regional presence of the data protection authority, together creating significant accountability gaps.

In Uganda, discrepancies between initial and final census reports raised serious questions about transparency. While corrected data was eventually released, it was done so without clear documentation explaining what had changed or why, an omission that served to undermine public trust in official statistics. In Tanzania, audit reports uncovered weaknesses in data management systems, including the use of generic user accounts and the presence of manual overrides that made it difficult, if not impossible, to trace data modifications.



These practices fundamentally compromised the reliability and auditability of government records. Some of the examples shared to demonstrate what weak data governance could lead to included:

- Loss of public trust
- Reduced accountability
- Increased potential for errors and bias
- Concentration of analytical power among a small group of expert

To address these challenges, Samo introduced the East African Reproducible Analysis Protocol (EARAP), a practical framework designed to promote transparency and reproducibility in data analysis across the region. The framework proposed a tiered approach to reproducible analysis enumerated below.

Foundation Tier which was the basic level applicable to all projects included:

- Maintaining an analysis log
- Saving final datasets in accessible formats
- Creating clear folder structures
- Providing documentation such as ReadMe files

Good Practice Tier- This tier involves:

- Saving code scripts used in analysis
- Documenting software versions
- Using syntax-based tools such as STATA, SPSS syntax, or R scripts

Gold Standard Tier- The most advanced level includes:

- Fully reproducible dynamic documents
- Version control systems such as Git
- Public code repositories with digital object identifiers (DOIs)

The framework also integrates guidelines for documenting AI-assisted analysis, including saving prompts and recording model versions to ensure transparency.

Call to Action

- Samo emphasized that improving data governance required collaboration among multiple stakeholders:
- Policymakers should mandate reproducibility standards in policy-related data analysis.
- Academic institutions should incorporate reproducible analysis practices into research training.
- Data practitioners should adopt transparency as a professional norm.

Ultimately, strengthening data governance required a cultural shift toward openness, accountability, and verifiable evidence. The session concluded with an interactive discussion between participants and the presenters. Participants asked how the EARAP framework would be validated and adopted across institutions in Africa. It was noted that EARAP was designed as a practical and adaptable framework rather than a rigid regulatory tool. Its validation be done through pilot implementation in research institutions, government agencies, and data projects across the region. Through real-world application, the framework could be refined based on user experiences and contextual challenges. The presenters also noted that building a community of practice among data practitioners would be key to ensuring its credibility and long-term adoption. Participants also asked what stakeholders consider the most urgent priority in ethical data governance. The presenters highlighted that safety, security, and data privacy currently rank as the most pressing ethical concerns, particularly due to increasing risks of data breaches and cyber threats. Transparency in AI systems and improved digital literacy were also identified as critical areas requiring attention. However, the discussion emphasized that ethical guidance must extend beyond technical safeguards to include fairness, transparency, and accountability in data-driven decision-making.

1. The breakout session highlighted the growing importance of evidence-based data governance in Africa's digital transformation. While technologies such as artificial intelligence offered significant economic opportunities, they also introduced new governance challenges that required robust institutional responses. The presentations underscored two key messages i.e. empirical evidence was essential for understanding how emerging technologies were used and governed in African contexts.

2. Second, transparent and reproducible analytical practices were critical for ensuring accountability in data-driven policymaking. Frameworks such as EARAP provided a promising pathway for strengthening transparency and trust in data systems. However, achieving meaningful progress would require collaboration among governments, researchers, civil society, and data practitioners to embed integrity, transparency, and accountability at the core of Africa's digital governance ecosystem.

Track 4: Ethics, Algorithms, and Accountability

Title: Beyond the Black Box: Safeguarding Regional Data Systems

Lead Organization: UNESCO

This breakout session focused on the governance challenges associated with algorithmic systems and artificial intelligence. Participants explored how automated decision-making systems increasingly shape public services, financial systems, and digital platforms across the region. A major concern raised was the lack of transparency in many algorithmic systems with most of the speakers noting that when algorithms function as “black boxes,” it became difficult for regulators, civil society, and citizens to understand how decisions affecting them are made.

Speakers highlighted some of the risks including:

- Algorithmic bias and discrimination
- Lack of transparency in automated decision-making systems
- Weak oversight of artificial intelligence applications
- Limited regulatory capacity to audit algorithms.

Key take aways:

- 1. Harmonizing of policies to access data.
- 2. Safety mechanism includes data minimization (specific data) oversight and accountability.
- 3. Policy infrastructure should be human-centered policy designed framework.
- 4. The measure of good governance is not how much advanced technology is, but how much is it helping the end user.



From Right: Angela Minayo, John Okande(UNESCO), Miriam Wanjiru(Public Policy Practitioner), Daniel Odongo(USHAHIDI), Rachel Olpengs(FECoMO)

Track 5: Economics & Value of Data (Monetization & Shared Benefit)

Title: Operationalizing Urban Data Governance in Eastern Africa through Data

Lead Organization: Toro Development Network

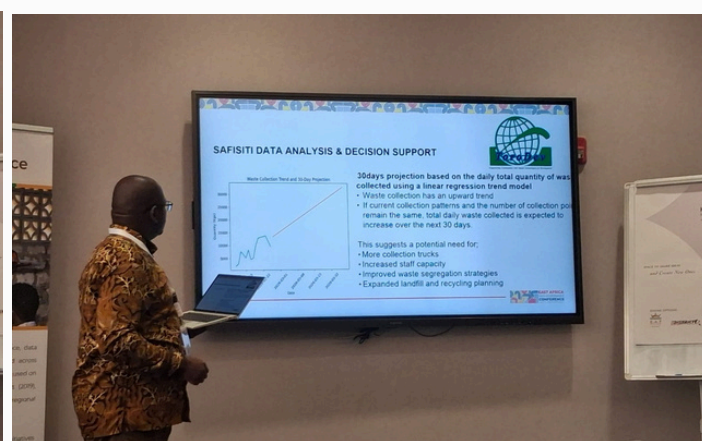
The second breakout session focused on practical approaches to operationalizing urban data governance through real-world applications. The presentation, delivered by Johnstone Baguma, examined how African cities could move beyond compliance-driven data protection frameworks toward governance models that leveraged data as a tool for development and improved urban service delivery. Drawing from experiences in emerging cities in Uganda, the presenters illustrated how governance principles could be embedded into digital systems that support evidence-based decision-making and accountability in city management. The session began by highlighting the progress made across Eastern Africa in establishing legal and institutional frameworks for data governance.

Countries such as Kenya, Uganda, and Tanzania had adopted comprehensive data protection legislation and established regulatory authorities responsible for overseeing the protection of personal data. Despite these developments, the presenters observed that most governance approaches remained largely compliance-oriented, focusing primarily on consent management, risk mitigation, and preventing data misuse. While these safeguards were necessary, they often limited the ability of governments to use data as a development asset. As a result, a gap had emerged where governance frameworks emphasized protection but did not sufficiently enable the use of data to drive innovation, economic growth, and improved public service delivery.

The presenters therefore emphasized the importance of adopting a balanced model of data governance that integrated ethical responsibility with development value. In this approach, data governance was not seen as a trade-off between privacy and innovation but rather as a framework that ensured both could coexist. Data played a crucial role in enabling evidence-informed planning and policymaking, improving the efficiency of urban services, and strengthening transparency and accountability in public administration. For instance, well-governed data systems could help cities optimize revenue collection, improve waste management logistics, support tourism development strategies, and enhance urban planning processes. Transparent data ecosystems could also attract investment and encourage digital innovation by providing reliable and predictable data environments.

To translate these principles into practice, the presenters introduced the use case approach to urban data governance. This model links governance frameworks directly to real urban challenges, allowing stakeholders to understand how governance mechanisms functioned in practical settings rather than as abstract policy concepts. By focusing on specific urban problems, city authorities could co-design digital systems that addressed operational challenges while embedding governance safeguards such as defined data ownership, access control mechanisms, and accountability structures. This approach also strengthened institutional ownership because city authorities became active participants in the design, implementation, and management of the data systems that supported their operations. The DataCities Initiative was presented as an example of how the use case approach could be implemented in practice. Working with emerging cities in Uganda, particularly Jinja and Fort Portal, the initiative identified priority urban challenges and collaborates with local stakeholders to develop digital systems that addressed them. These systems are designed in alignment with governance principles and national data protection frameworks while also institutionalizing reporting, accountability, and policy linkages. Through this model, data governance would be integrated into routine city operations rather than remaining a purely regulatory concept.

A key example highlighted during the presentation was the SafiSiti urban waste management platform, a digital system developed to improve waste management governance in participating cities. Prior to the introduction of the platform, city authorities faced several challenges including limited visibility of waste generation volumes, fragmented reporting by private waste collectors, and weak monitoring of service coverage. These challenges resulted in inadequate data for planning waste management strategies and limited oversight of waste collection services.





SafiSiti as a Practical Data Governance Model

SafiSiti addresses these issues by digitizing waste data collection and reporting, enabling city authorities to track waste volumes, monitor collection performance, and map waste generation patterns spatially across urban areas. It demonstrates how digital platforms could embed governance principles directly into operational systems. The platform incorporated standardized reporting indicators, clearly defined data ownership structures, role-based access controls, and structured data-sharing protocols. Digital audit trails ensured that transactions and activities within the system were traceable, strengthening transparency and oversight in urban service delivery. Through its data dashboard, city authorities could analyze waste collection routes, identify underserved areas, track recycling rates, and monitor contractor performance. Predictive data analysis also enabled cities to anticipate increases in waste generation and plan accordingly by adjusting staffing, logistics, and infrastructure capacity. Importantly, the platform integrated safeguards that ensured that urban data governance remained aligned with privacy and ethical standards.

These safeguards included data minimization, aggregated reporting, secure hosting protocols, and consent mechanisms where household-level data was involved. The system focused on operational and spatial data rather than personal surveillance, reinforcing trust among citizens while still enabling valuable insights for decision-making. The presenters concluded by noting that implementing digital urban data systems raised important governance questions, particularly regarding data ownership, data-sharing frameworks, and reporting obligations between city authorities, technology providers, and private service contractors. Addressing these issues required clear governance agreements and collaborative oversight mechanisms noting that effective data governance was not only about protecting data but also about responsibly unlocking its value for inclusive urban development. By embedding governance principles into practical digital systems, cities could improve service delivery, strengthen accountability, and create new opportunities for sustainable economic growth.

Track 4: Ethics, Algorithms, and Accountability

Title: Digital Dignity: Putting people at the Centre of Humanitarian Data in East Africa

This breakout session, led by MSF Eastern Africa, examined the ethical challenges surrounding humanitarian data collection and management, emphasizing the need to place human dignity at the center of digital systems used in crisis response. The discussion highlighted how humanitarian organizations increasingly relied on data to guide interventions, yet the processes used to collect, manage, and interpret that data often lacked sufficient safeguards to protect the individuals and communities from whom the data originated. A central theme of the discussion was the widespread practice of overcollection of data with observation to the effect that civil society and humanitarian organizations often collected information that extended beyond the original scope of their data-gathering exercises. For instance, while data collection may begin with a specific objective such as identifying vulnerable households, enumerators frequently gathered additional information about household economic conditions, employment status, or living environments. While such information could be useful for contextual analysis, it also raised concerns about privacy, consent, and whether organizations were operating within clearly defined data governance boundaries.

The discussion emphasized the need for humanitarian organizations to reframe their role from data owners to temporary custodians of sensitive information. This shift recognizes that the data collected represents real individuals whose privacy, security, and agency must be protected. Participants stressed that data should only be used for the purpose for which it was originally collected, and that organizations must ensure responsible stewardship throughout the data lifecycle from collection and storage to analysis and eventual deletion. Participants further raised concerns about the lack of clear institutional policies guiding data governance in humanitarian settings, particularly for organizations operating in crisis contexts across multiple countries. Questions were raised about whether international humanitarian organizations should establish stronger internal governance structures or centralized offices responsible for overseeing data protection and ensuring compliance with both international standards and national data protection laws.



The role of community participation in data collection was another key issue discussed for example in many humanitarian contexts, community members themselves are engaged as enumerators or data collectors. While this approach could improve trust and accuracy, given that communities often had deep knowledge of local demographics, such as the number of households or families with young children, it also introduced ethical responsibilities. Participants emphasized that community data collectors must be trained to handle sensitive information appropriately and that mechanisms should be in place to ensure that data was held only in temporary, secure states before being transferred to protected systems. The conversation further highlighted the growing use of digital tools and artificial intelligence in humanitarian data analysis, which introduced new ethical considerations. Participants noted that algorithms used to analyze or filter large datasets could unintentionally reproduce or amplify biases embedded within the data. As such, organizations must invest in building the capacity of their staff to critically assess AI-generated outputs, identify potential biases, and implement corrective measures to ensure equitable and fair decision-making.

To address these challenges, the session underscored the importance of establishing robust governance frameworks, secure digital systems, and institutional accountability mechanisms including training staff on the ethical use of data collection tools, implementing strong data storage and monitoring systems, and ensuring compliance with national data protection regulations. Participants also emphasized the value of inter-organizational networks and coordination, noting that collaboration between humanitarian actors could strengthen shared standards, improve data protection practices, and reduce duplication in data collection efforts.

Overall, the discussion reinforced that upholding digital dignity required a fundamental shift from a mindset of data extraction to one of responsible stewardship. In humanitarian contexts, where affected populations may already face heightened vulnerability, safeguarding their data was not only a technical responsibility but also an ethical imperative.

Key Outcomes & Recommendations from this session included:

1. Privacy by Design and by Default: Humanitarian organizations should embed privacy protections into digital systems from the outset, ensuring that safeguarding personal data was an integral part of program design and implementation.
2. Data Minimization: Organizations should limit data collection strictly to information necessary for delivering humanitarian assistance, avoiding the routine gathering of additional or unrelated personal data.
3. Strengthened Data Governance Frameworks: Humanitarian actors should establish clear institutional policies and governance mechanisms that guided responsible data collection, storage, sharing, and deletion, while aligning with national data protection laws.
4. Capacity Building for Ethical Data Use: Staff and community data collectors should receive training on responsible data management, including the ethical use of digital tools and the identification of potential algorithmic bias in AI-supported analysis.
5. Community-Centered Data Practices: Engaging communities in data collection should be accompanied by safeguards that protect data subjects and ensure that community enumerators understand confidentiality, consent, and secure data handling.
6. Improved Coordination and Learning: Strengthening networks and collaboration among humanitarian organizations can support the development and scaling of best practices in ethical data governance across crisis contexts.

Lighting talks

Two lightning talk presentations were delivered highlighting upcoming global data initiatives and practical experiences in improving the usability of data systems for policymaking

Presentation 1: Pitch- 2026 Global Data Festival and Kenya Space Expo & Conference

Speaker: Jenna Slotin (Global Partnership for Sustainable Development Data – GPSDD)



Jenna introduced the upcoming 2026 Global Data Festival, which will be held in Nairobi from 2–5 June 2026 alongside the Kenya Space Expo and Conference. The event is organized in collaboration with the Government of Kenya, the UN Tech Envoy's Office, the Kenya Space Agency, and the Kenya National Bureau of Statistics, and is designed to convene global stakeholders working at the intersection of data governance, innovation, and emerging technologies. She emphasized that the current global moment marked by rapid technological advancement, the expansion of artificial intelligence, and evolving geopolitical dynamics required stronger collaboration and new forms of partnership. The Global Data Festival aimed to create a space where practitioners, policymakers, and innovators could co-create actionable ideas, form coalitions for change, and develop practical tools that could be applied in their respective contexts.

A key theme of the presentation was the importance of partnership and collaboration across ecosystems. By hosting the festival jointly with the Kenya Space Expo, the event would bring together communities working in data governance, artificial intelligence, earth observation, and space technologies. This integrated approach was intended to foster interdisciplinary solutions and encourage knowledge exchange among actors working across the data and technology landscape. Jenna noted that Kenya represented a strong example of digital innovation and leadership in the region which greatly influenced its hosting of this event. From its reputation as the “Silicon Savannah” to its efforts in developing national AI strategies and advancing digital governance frameworks, Kenya provided a dynamic context for global discussions on the future of data governance. Participants were encouraged to attend the event, share information with their networks, and engage with the festival's collaborative opportunities. The festival is expected to attract participants from across Africa and globally, providing a platform for dialogue, networking, and the development of partnerships aimed at advancing data-driven solutions for sustainable development.

The Duality of Dashboards: Balancing Data Complexity and Policy Usability

Speaker: Winnie Awor – Development Gateway

Winnie Awor presented on the duality of dashboards, focusing on the challenge of balancing complex data systems with the need to make information accessible and useful for policymakers. Drawing from Development Gateway's work across sectors such as public health and agriculture, she explained how dashboards could serve as practical tools for translating large volumes of data into actionable insights. She highlighted several challenges commonly encountered in the development of data dashboards. One major issue was that data was often scattered across multiple sources and presented in formats that were difficult for policymakers to interpret. In many



cases, critical evidence remained buried within lengthy reports that were rarely consulted, limiting their usefulness for decision-making. Another challenge arose from the mismatch between data availability and policy needs. Data collected many years earlier may not reflect current realities, making it difficult for policymakers to rely on it when designing new policies or interventions.

Additionally, policymakers frequently faced difficulties in determining which data sources were most credible, particularly when industry-produced data may conflict with independent research findings. To address these challenges, Development Gateway adopts an iterative and collaborative approach to dashboard development. Stakeholders, particularly government ministries and agencies, are involved from the earliest stages of the process. This includes identifying key data needs, validating information with subject matter experts, and co-designing dashboards that reflect real policy priorities. By engaging stakeholders throughout the process, institutions develop a stronger sense of ownership over the platforms and are more likely to use them in their work. Awor also emphasized the importance of ensuring that dashboards remain practical tools rather than static information repositories. Beyond building the platforms, Development Gateway conducts follow-up engagement and impact assessments with ministries and civil society organizations to understand how the dashboards are being used and whether they are informing policy discussions. Examples were shared demonstrating how dashboard-generated insights have supported policy advocacy. In the Democratic Republic of Congo, newly collected data on illicit tobacco trade helped policymakers build evidence to support discussions on ratifying an international protocol addressing illicit tobacco products. In other countries such as Kenya, Zambia, and South Africa, civil society organizations have used dashboard insights and accompanying policy briefs to engage policymakers and strengthen arguments during legislative discussions. Awor concluded by emphasizing the need for greater investment in locally generated data and more accessible dissemination formats. Instead of relying solely on lengthy technical reports, data should be translated into dashboards, policy briefs, and other formats that allow decision-makers to quickly understand and apply evidence in policy processes. By making data more accessible and actionable, dashboards can play a critical role in bridging the gap between complex data systems and effective policymaking.

BREAKOUT SESSION 2

Track 1: Data Ownership and Custodianship, Data Sovereignty

Title: Haki Yako Mtandaoni: Emerging issues on Data Protection and Digital Rights among the Youth in Kenya: Open Institute

This session presented the findings and evolution of the #FichaUchi awareness campaign, an Open Institute initiative dedicated to educating citizens in Kenya, Uganda, and Tanzania on data privacy and their rights under national Data Protection Acts. The discussion focused on the unique vulnerabilities of young people in the digital space and the critical role of civil society in bridging the gap between policy enactment and public awareness. The session opened by framing the problem: while Kenya passed its Data Protection Act in 2019, a 2020 opinion poll by Amnesty International Kenya revealed that 54% of Kenyans were unaware of their right to privacy. This awareness gap left citizens vulnerable to data misuse and unable to exercise their rights. In response, the #FichaUchi campaign was launched in 2021 to educate citizens on what the Data Protection Act means for them, their rights and responsibilities, and the steps they can take if their data is misused. The presentation underscored the importance of focusing on young people, highlighting that:

- Youth are the largest digital users in Kenya, with 31% of the 18-24 age group using the internet daily.
- Despite high usage, there is a significant lack of awareness, exposing them to risks of exploitation, scams, and identity theft.
- The session framed digital rights as human rights in the online space, emphasizing that protections must extend to digital environments.

The Open Institute identified several persistent challenges facing young people in East Africa including:

- Oversharing of personal information on social media.
- A limited understanding of dense and often inaccessible data privacy policies.



- High exposure to scams and phishing attacks.
- Inadequate digital literacy education in school curricula.
- Unequal access to information about digital rights, particularly for marginalized youth.

A key focus of the session was the campaign's strategic evolution. Recognizing that a purely digital campaign could not reach everyone, #FichaUchi expanded into Phase 2: #FichaUchi 2.0. This phase moved beyond social media to include on-the-ground engagement, reaching an estimated 115 million people through:

- A sustained digital campaign.
- Community radio talk shows across nine countries.
- Focus groups engaging over 200 young people in Tanzania and Uganda to understand their lived experiences with data privacy.

The Role of Civil Society and Persistent Gaps

The session concluded with a critical reflection from a civil society perspective on the gaps that exist in protecting young people's data:

1. Awareness vs. Understanding: While campaigns have raised awareness, deep understanding of privacy policies and technical safeguards remained low.
2. Policy Accessibility: Data protection laws and policies are often not communicated in language or formats that were accessible to young people.
3. Digital Literacy: There is an urgent need to integrate digital rights and data privacy into formal education, rather than relying solely on ad-hoc campaigns.
4. Feedback and Redress: Young people often do not know how or where to report data misuse, and accountability mechanisms remain opaque.

Key Recommendations

Based on the findings from the #FichaUchi campaign, the session offered the following recommendations for strengthening data protection and digital rights among youth:

- Move beyond social media: Effective awareness campaigns must complement digital outreach with on-the-ground engagement, including community radio and in-person focus groups, to reach those with limited internet access.
- Integrate digital literacy into education: Governments and education partners should prioritize integrating data privacy and digital rights into school curricula to build foundational knowledge from an early age.
- Make policies accessible: Data protection policies must be translated into youth-friendly formats and local languages to ensure they are understood by those they are designed to protect.
- Strengthen accountability mechanisms: Clear, accessible channels for reporting data misuse must be established and communicated, ensuring that rights are not just theoretical but enforceable.
- Sustain engagement: One-off campaigns are insufficient. Continuous, evolving engagement like the shift to #FichaUchi 2.0, is necessary to keep pace with changing technology and emerging risks.





Track 2: Sovereignty and Cross-Border Governance

Title: Safeguarding Rights in Synthetic Media in EA: Ethical AI, Personal Data, and Creative Ownership: Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University.

Moderated by: Joshua Kitili (AI Governance and Technology Law Expert)

Panelists

- Francis Monyango – Group Data Protection Officer, Old Mutual (Africa)
- Chebet Koros – Intellectual Property Researcher, CIPIT (Centre for Intellectual Property and Information Technology Law)
- Richard Odongo – Senior Associate, Intellectual Property & Technology Law
- Quency Otieno-AI governance and systems expert

Session Overview

This breakout session took the form of a panel discussion examining the legal, ethical, and governance challenges posed by synthetic media and artificial intelligence in East Africa. The discussion focused on the intersection of AI model development, personal data protection, intellectual property rights, and accountability frameworks in the context of rapidly evolving generative technologies. The conversation highlighted that while artificial intelligence systems increasingly generate synthetic media including deepfakes, AI-generated artwork, and automated content existing legal frameworks in many African jurisdictions have not fully caught up with the realities of these technologies. Panelists explored how current data protection laws, intellectual property regimes, and governance frameworks can be interpreted to address emerging risks while enabling responsible innovation.

Key Issues Discussed

1. AI Training Data and Intellectual Property Risks

One of the central themes discussed was the use of copyrighted data in training AI systems. Panelists noted that generative AI models rely heavily on large datasets containing text, images, and other creative works, many of which may be protected by copyright. Chebet Koros explained that traditional copyright frameworks assume that creative works are produced by human authors, which complicates questions about ownership of AI-generated content. Because copyright protection automatically vests in human creators, the legal status of works generated entirely by AI remains uncertain. She noted that this creates complex questions around authorship, attribution, and moral rights, particularly when AI systems replicate artistic styles or generate content derived from copyrighted datasets.

“Copyright law was designed around a human author. When AI generates content using large datasets, the question becomes: who actually owns the output?”

Panelists also discussed the possibility that AI-generated works may fall into the public domain if human authorship cannot be demonstrated, though this interpretation varies across jurisdictions and remains contested in many policy debates.

2. Personal data scraping and privacy concerns

The panel also examined how AI systems collect and process personal data, particularly through automated data scraping techniques used to train machine learning models. Francis Monyango highlighted that under Kenya’s Data Protection Act, personal data should ideally be collected directly from the data subject. However, the law also allows certain exceptions where data may be collected indirectly, particularly when the information has already been made publicly available. This creates a regulatory grey area in the context of AI training, where personal images, social media posts, or publicly accessible content may be scraped and incorporated into datasets without explicit consent from the individuals concerned.



Once information is made public online, the law allows certain forms of indirect collection. That creates a complex space when AI systems scrape data to train models.

Panelists noted that while consent remains an important principle in data protection law, the scale and automation of AI data collection challenge traditional notions of informed consent and user control over digital identity.

3. **Synthetic media and the growing challenge of deepfakes**

Another major concern raised during the discussion was the rapid advancement of synthetic media technologies, particularly deepfakes. Panelists explained that improvements in machine learning techniques such as reinforcement learning have significantly increased the realism of AI-generated images and videos, making it increasingly difficult to distinguish between authentic and synthetic content. This technological evolution raises serious concerns for misinformation, reputational harm, and political manipulation, especially in contexts where synthetic media can be used to distort public narratives or misrepresent individuals. Panelists emphasized the importance of building detection mechanisms, digital literacy, and stronger governance frameworks to address these risks.

4. **Accountability in the AI Ecosystem**

A key governance question discussed during the panel was who should be held accountable when AI systems cause harm. Panelists debated whether responsibility should lie primarily with developers, deployers, platforms, or end users. Quency suggested that accountability in AI systems should be distributed across multiple actors, rather than assigned to a single stakeholder. Because AI systems operate through complex ecosystems involving developers, platforms, and users, liability should depend on how the technology is designed and used. Developers, for example, may bear responsibility if systems are designed without adequate safeguards, while users may also share responsibility if they deliberately misuse AI tools to generate harmful content. This layered accountability approach reflects emerging governance models being discussed globally, including in frameworks such as the EU AI Act, which categorizes risks and assigns responsibilities across different actors within the AI value chain.

5. **Cross-Border enforcement challenges**

Panelists also addressed the difficulty of enforcing intellectual property rights and data protection laws when AI systems operate across national borders. Richard Odongo explained that while copyright protection is automatically granted to creators under many legal systems, enforcing those rights becomes far more complicated when AI systems trained on copyrighted data are developed or deployed in different jurisdictions. Regional and international frameworks such as WIPO conventions and regional IP systems provide some mechanisms for cooperation, but these systems were not originally designed to address disputes involving AI-generated content or cross-border AI training datasets. As a result, creators may face significant challenges in identifying responsible parties and pursuing legal remedies when their works are used in AI training without authorization.

Governance Priorities Highlighted by the Panel

Several key governance priorities emerged from the discussion:

- Clarifying the application of existing intellectual property laws to AI-generated works and training datasets.
- Developing regulatory guidance for AI developers and data users on how current laws apply to emerging technologies.
- Strengthening accountability mechanisms across the AI lifecycle, including development, deployment, and use.
- Enhancing transparency in AI training datasets, particularly where copyrighted works or personal data are involved.
- Promoting digital literacy and public awareness to help citizens identify and respond to synthetic media threats.



Panelists emphasized that while existing laws provide a starting point for addressing these issues, legal reforms and clearer regulatory guidance will likely be necessary to ensure that intellectual property rights, privacy protections, and creative ownership are adequately safeguarded in the age of artificial intelligence. The panel underscored that synthetic media and generative AI are rapidly transforming the digital ecosystem, raising complex legal and ethical questions about ownership, privacy, and accountability. While East African countries have made progress in developing data protection and intellectual property frameworks, these laws must evolve to address the realities of AI-driven content creation and automated data processing.

Ultimately, safeguarding rights in the age of synthetic media will require multi-stakeholder collaboration among policymakers, technologists, legal experts, and civil society to develop governance frameworks that both protect individual rights and support innovation in the region's growing digital economy.

Track 4: Ethics, Algorithms, and Accountability

Title: When Data Harms Defenders: Rebuilding Accountability in East Africa's Data Systems Led by Noelyn Nassuuna- Defenders Protection Initiative



This session examined how emerging data systems and algorithmic technologies were reshaping the risk environment for human rights defenders, journalists, and civil society actors across East Africa. Participants explored how the expansion of digital identification systems, biometric databases, predictive analytics, and algorithm-driven monitoring tools could unintentionally or deliberately be used to track, profile, or restrict civic actors when adequate safeguards were not in place. Civil society representatives shared examples demonstrating how personal data, digital communications, geo-location information, and online activity had been used to monitor or target activists and investigative journalists. Participants

emphasized that defenders often operated in politically sensitive environments where access to digital platforms and communication tools was essential for organizing, documentation, and advocacy. When these digital traces are collected or analysed without transparency or consent, they can expose defenders to harassment, intimidation, travel restrictions, or legal action. The discussion also focused on the ethical challenges posed by automated decision-making systems and opaque algorithms used in security, governance, and digital service delivery. Participants noted that algorithmic systems trained on incomplete or biased datasets may reinforce existing inequalities or disproportionately flag individuals and organizations engaged in civic activism. The lack of transparency in how these systems function makes it difficult for affected individuals to challenge decisions or seek remedy.

Another key theme was the growing role of private technology companies in collecting, processing, and storing large volumes of data. Participants highlighted the need for clearer accountability frameworks governing public-private partnerships in data infrastructure, particularly where private firms manage digital identity systems, telecommunications data, or surveillance technologies on behalf of governments. The session further highlighted the limited digital security resources available to many civil society organizations and grassroots movements. Without adequate knowledge of data protection practices, encryption tools, and secure communications, defenders remain vulnerable to data breaches, unauthorized monitoring, and cyber harassment.

Key discussions included:

- The need for stronger safeguards for sensitive personal data, particularly data related to civic engagement, political participation, and human rights work.
- Legal protections for whistleblowers, journalists, and human rights defenders who expose misuse of digital systems or data-driven abuses.
- Establishing independent oversight mechanisms for surveillance technologies such as facial recognition, digital tracking tools, and large-scale monitoring systems.

- Strengthening accountability frameworks that apply to both state institutions and private technology actors involved in data collection and processing
- Promoting transparency and explain ability in algorithmic systems used in governance and public service delivery
- Supporting civil society capacity-building on digital security, ethical data practices, and responsible data governance

Participants emphasized that accountability in data systems must go beyond technical safeguards and include meaningful participation of civil society in policymaking processes related to digital governance. Transparent regulatory frameworks, human rights impact assessments, and accessible complaint and redress mechanisms were identified as essential components of responsible data governance. The session concluded that protecting defenders in the digital era requires comprehensive data governance frameworks grounded in human rights principles, transparency, and accountability. Participants called for stronger regional collaboration among governments, civil society organizations, and oversight institutions to ensure that digital transformation across East Africa strengthens democratic participation rather than undermining civic freedoms.

Plenary Panel 2: Building Trust: What Will it Take to Govern Data for All?

Private sector panel: KCB, Smart Applications Group, Google, UoN, Safaricom Ltd

The second plenary panel, and last session of the day examined how trust could be built within modern data ecosystems, particularly as private sector actors increasingly play a central role in collecting, managing, and analyzing large volumes of personal and institutional data. Moderated by John Mburu of Expertise Global, the panel brought together representatives from technology companies, financial institutions, health technology providers, and academia. Panelists included Michael Murungi (Google), Rosemary Koech (Kenya Commercial Bank), Joshua Chepkwony (Smart Applications Group), Dr. Benard Wanjohi (University of Nairobi), and a representative from Safaricom Ltd responsible for Business Intelligence and Data Governance.



Michael Murungi (Google), Rosemary Koech (Kenya Commercial Bank), Joshua Chepkwony (Smart Applications Group), Dr. Benard Wanjohi (University of Nairobi)

The discussion highlighted the growing importance of responsible data stewardship, ethical governance, and interoperability as essential foundations for trust in digital systems. While digital technologies had the potential to transform service delivery across sectors such as finance, healthcare, and telecommunications, panelists emphasized that the success of these systems ultimately depended on the confidence citizens have in how their data is collected, processed, and protected.

Private sector representatives emphasized that trust must be embedded into digital systems from the earliest stages of development rather than treated as an afterthought once technologies were deployed. The representative from Safaricom explained that privacy and security considerations were integrated directly into the company's product development processes. Whether systems were developed internally or procured from external vendors, Safaricom applied baseline technical, privacy, and security standards before systems were allowed to move into production.



These safeguards include data minimization, encryption, and role-based access controls to ensure that information remained protected both at rest and during transmission. The representative described this approach as “shifting security and privacy left,” a model in which governance safeguards are incorporated early in the design and architecture of digital platforms.

Joshua Chepkwony of Smart Applications Group reflected on the challenges associated with managing highly sensitive health data within digital systems. Smart Applications operated platforms used by insurance providers and hospitals to process medical claims and manage health records, meaning the organization handled some of the most sensitive forms of personal data. Chepkwony emphasized that protecting such data could be treated as a purely technical responsibility but must be embedded within broader organizational governance structures. At Smart Applications, data protection issues were discussed at the board level to ensure strategic oversight. The company also integrated data protection responsibilities into employee performance indicators and conducted regular internal awareness initiatives to strengthen staff understanding of privacy obligations. These efforts aimed at cultivating a culture of accountability around data stewardship. From the financial sector perspective, Rosemary Kuria of Kenya Commercial Bank discussed how financial institutions managed personal data within highly regulated environments. Banking services relied heavily on personal information, including identity verification data, financial transaction histories, and customer contact details. As a result, effective operations depended on strong governance systems that ensured personal data was handled responsibly. Kuria explained that financial institutions increasingly involved privacy professionals in technology development processes from the earliest stages of system design. Instead of reviewing digital systems shortly before deployment, privacy teams now participated in design and architecture reviews to ensure that regulatory requirements and ethical considerations were incorporated from the outset. She also highlighted the role of professional networks such as the Digital Privacy and Governance Society of Kenya in fostering collaboration among practitioners, regulators, and researchers to develop shared standards and best practices across sectors.

Dr. Benard Wanjohi of the University of Nairobi provided an academic perspective on the broader societal implications of data governance. He observed that while private sector organizations often view data as a strategic asset that enables innovation and commercial growth, citizens increasingly question how their data was used and whether they received fair value from its use. Wanjohi noted that one of the emerging governance challenges in the digital economy was the perception that organizations extracted large volumes of data without sufficient transparency or accountability. These concerns were particularly relevant in the context of big data and artificial intelligence, where extensive datasets may be collected and analyzed in ways that were not always visible to the individuals whose data was being used. He emphasized the role of academia in generating evidence and critical analysis that can help policymakers and industry leaders develop governance frameworks that balance technological innovation with public accountability.

Michael Murungi of Google reflected on the role that global technology companies played in strengthening digital infrastructure across Africa. He highlighted initiatives aimed at improving digital connectivity and supporting innovation ecosystems within the region. One example was the Umoja subsea cable project, which aimed to expand internet connectivity across East Africa and enhanced the resilience of regional digital infrastructure. By improving connectivity and reducing reliance on limited infrastructure routes, such investments can strengthen the reliability of digital services across multiple countries. Murungi also noted efforts to improve the representation of African languages and contexts within artificial intelligence systems through research initiatives focused on developing inclusive datasets. These efforts were intended to ensure that AI technologies developed globally can function effectively within African environments.

The panel also explored the importance of interoperability in building effective regional data ecosystems. Interoperability allows digital systems such as financial platforms, healthcare databases, and digital identity infrastructures to communicate and exchange information seamlessly. Panelists observed that without shared standards and coordinated governance frameworks, digital systems risked becoming fragmented, limiting their ability to deliver integrated services. In the healthcare sector, for example, lack of interoperability often meant that patients must repeat diagnostic tests when visiting different hospitals because digital medical records cannot easily be shared between systems.

Addressing such challenges required collaboration among governments, private sector actors, and regional institutions to establish harmonized standards that allowed digital systems to function across institutional and national boundaries. The panel discussion generally underscored that trust in digital ecosystems depended on transparent governance frameworks, responsible data stewardship, and collaboration among multiple stakeholders. Embedding privacy and security safeguards into the design of digital systems, strengthening institutional accountability, investing in digital infrastructure, and promoting interoperable governance frameworks were identified as essential steps toward building resilient and trustworthy data ecosystems across East Africa.

Photo gallery



Badge collection by the conference delegates



Press briefing led by Immaculate Kassait, Data Commissioner, Office of the Data Protection Commissioner, Kenya



Light moments at the conference



The conference ensured all sessions had a sign language interpreter



Networking moments by participants



Group photo of conference organizers from Open Institute and Amnesty Kenya together with key dignitaries including the Regional Data Protection leaders from Kenya, Uganda and Tanzania

Day 2

Opening and climate setting

The second day of the East Africa Data Governance Conference 2026 began with an interactive and energizing session designed to re-engage participants while reinforcing the regional identity that underpins conversations on data governance in East Africa. The session was facilitated by the conference moderator, who set an engaging tone through a series of interactive activities aimed at fostering participation and community among attendees.



Recap of Day One

As part of the recap for day two Victor Ndede welcomed participants back and acknowledged the strong participation on the first day of the conference. He highlighted that the forum had already hosted a range of insightful discussions bringing together policymakers, researchers, civil society actors, and private sector representatives working in the data governance space across the region. He then provided a brief recap of key highlights from Day One, including:

- Opening remarks delivered by conference organizers and partners
- A keynote address by Immaculate Kassait, Kenya's Data Protection Commissioner, which explored the balance between innovation and accountability in data governance
- A high-level panel discussion examining how governments, private sector actors, and civil society can strike this balance in practice

Victor also highlighted the wide range of breakout sessions and thematic discussions that took place during the first day, which addressed diverse aspects of data governance, including:

- Data ownership and inclusive governance, examining whose data counts and how participation and power shape governance frameworks
- Data-driven decision-making in social protection, particularly how data systems influence access to care and public services
- Evidence and accountability in data governance, led by the Centre for the Study of the Economies of Africa
- Freedom of expression online, facilitated by UNESCO and the Coalition on Freedom of Expression Online
- Urban data governance, with insights from emerging city data initiatives in Uganda presented by Toro Development Network
- Humanitarian data governance, led by Médecins Sans Frontières (MSF) focusing on placing people at the center of humanitarian data systems in East Africa
- Lightning talks by the Global Partnership for Sustainable Development Data linked to the Global Data Festival
- A session by Centre for Intellectual Property and Information Technology (CIPIT) law at Strathmore University exploring the governance implications of synthetic media
- Discussions on data harms faced by human rights defenders, led by the Defenders Protection Initiative
- A closing plenary featuring private sector perspectives on what it will take to govern data for all.



Participants were informed that the second day would continue exploring the conference theme through five thematic tracks, with particular attention given to data ownership and custodianship. This track examines critical questions about who owns data, who controls it, and who ultimately benefits from its use. As the opening session transitioned into the keynote segment, Mr. Kisaka, the moderator reflected on insights from the previous year's conference. One of the central takeaways was that data governance is not only about systems, regulations, and technologies, but fundamentally about people.

Building on that reflection, he reminded the participants of the contributions made by Melissa Omino, who had in last year's data governance conference, challenged audiences to move beyond compliance-driven approaches to data governance and instead consider deeper questions around power, participation, and representation. The keynote for day two would be delivered by Melissa Omino, Director of the Centre for Intellectual Property and Information Technology Law at Strathmore University. Dr. Omino was introduced as a leading scholar in digital rights, artificial intelligence governance, and technology policy in Africa. Her work bridges the gap between academic research and policy engagement, positioning her institution as both a research center and a policy think tank working on issues related to:

- Artificial intelligence governance
- Data governance frameworks
- Intellectual property
- ICT law and digital policy

Keynote by Dr Melissa Omino, Executive Director, Centre for Intellectual Property and IT Law (Strathmore University)

Topic: Before the Dataset: The Human Story behind Governance

Building on reflections from the previous day's discussions, Dr. Omino challenged participants to rethink conventional approaches to data governance by placing communities, cultures, and lived experiences at the center of policy and technological development. Her keynote highlighted several critical themes shaping the future of data governance in East Africa.

- **Human-centered data governance:** Dr. Omino emphasized that effective data governance must begin with people rather than systems. Digital datasets were ultimately derived from the experiences, knowledge, and realities of communities, and governance frameworks must therefore reflect these social and cultural contexts. She warned that when governance systems overlooked this relationship, they risked prioritizing technical efficiency over human rights and social justice.
- **Language and representation in data systems:** A major concern raised during the keynote was the underrepresentation of African languages and cultural contexts in digital datasets and artificial intelligence systems. Dr. Omino cautioned that this gap risked reinforcing inequalities in digital technologies by excluding local knowledge and perspectives. She stressed the need for inclusive governance approaches that ensured African communities were not merely sources of data but active participants in shaping how data systems are developed and used.
- **Digital governance and civic participation:** Dr. Omino also reflected on how digital technologies were increasingly shaping civic participation and public discourse in the region. As digital platforms became key spaces for activism and democratic engagement, she emphasized that data governance frameworks must safeguard fundamental rights such as freedom of expression, privacy, and participation in digital civic spaces.
- **Balancing innovation and accountability:** The keynote further highlighted the need to ensure that technological innovation did not outpace regulatory safeguards. Dr. Omino called for stronger collaboration between regulators, civil society, and technology developers to ensure that innovation is aligned with public interest, democratic values, and human rights.



Plenary Panel 3: The “Value and Vulnerability” of Digital Public Infrastructure (DPI)

The first plenary panel of Day Two at the East Africa Data Governance Conference 2026 examined the opportunities and governance challenges associated with the rapid expansion of Digital Public Infrastructure (DPI) across the region. The session was moderated by Mark Irura. The panel brought together diverse perspectives from development partners, policy research institutions, and regulatory authorities, including Emmanuel Emurugat (Digital Transformation Centre, GIZ Kenya), Kwame Owino (Executive Director, Institute of Economic Affairs, Kenya), Paul Kakeeto (Public Relations and International Affairs Manager, Personal Data Protection Office Uganda), and Karen Bett (Program and Policy Lead, Global Partnership for Sustainable Development Data). The discussion explored the dual nature of digital public infrastructure as both a powerful enabler of digital transformation and a potential source of governance vulnerabilities. Panelists agreed that while investments in digital identity systems, digital health platforms, and payment infrastructure are accelerating across Africa, governance frameworks must evolve alongside these systems to ensure accountability, trust, and protection of citizens’ rights.



From left: Kwame Owino- Institute of Economic Affairs, Kenya; Paul Kakeeto-Personal Data Protection Office Uganda; Karen Bett- Global Partnership for Sustainable Development Data; Emmanuel Emurugat- (Digital Transformation Centre, GIZ Kenya); Mark Irura-CIPIT

Emmanuel Emurugat opened the discussion by clarifying the relationship between Digital Public Goods (DPGs) and Digital Public Infrastructure (DPI). He explained that digital public goods such as open-source software, digital health platforms, and interoperable payment systems, serve as reusable technological components that governments can adopt when building scalable digital services. These tools allow governments to deploy digital systems more efficiently by reducing duplication and enabling interoperability across sectors. However, Emmanuel cautioned that although technological solutions are often available, governance frameworks frequently lag behind technological implementation. Without strong institutional coordination and policy safeguards, digital infrastructure projects risk becoming fragmented or failing to gain public trust.

Karen Bett highlighted growing concerns among citizens regarding the increasing digitization of public services. Drawing from experiences within the Global Partnership for Sustainable Development Data network, she outlined three recurring issues raised by communities. First, citizens often question whether digital systems actually improved service delivery. Even when digital platforms were introduced to simplify processes such as civil registration or public service access, bureaucratic inefficiencies persisted, undermining confidence in the technology. Secondly, concerns about data privacy and security frequently arose with citizens wanting assurance that their personal data would not be misused, shared without consent, or exploited for surveillance purposes. Bett also noted that communities often felt excluded from the design of digital systems. She emphasized that meaningful participation must go beyond symbolic consultations and instead involve co-creation processes where citizens actively shaped digital infrastructure initiatives. While providing a political economy perspective, Kwame Owino observed that many governments were introducing large-scale digital systems at a time when public trust in institutions was already fragile. In such contexts, digital infrastructure projects may be perceived not as tools for improving service delivery but as mechanisms that could enable surveillance or political control.

Previous incidents involving the misuse of digital technologies such as monitoring protests or restricting media coverage further intensified public scepticism. Owino emphasized the need for governments to openly acknowledge both the benefits and risks of digital infrastructure initiatives. Building trust required transparent governance frameworks, strong safeguards, and inclusive participation in system design. From a regulatory standpoint, Paul Kakeeto discussed how data protection authorities could help balance innovation with privacy safeguards. Representing the Personal Data Protection Office in Uganda, he noted that many organizations and citizens still have limited awareness of data protection laws. To address this gap, the PDPO had introduced compliance support initiatives including toolkits that guided organizations in conducting data protection impact assessments, developing privacy policies, and managing cross-border data transfers. Kakeeto also highlighted ongoing work to strengthen regulatory frameworks through new guidelines on data breach notifications, privacy-by-design principles, and the designation of data protection officers within institutions. These measures aimed at ensuring that privacy protections were embedded into digital systems from the earliest stages of development. Most importantly, he emphasized that regulation should not be viewed as a barrier to innovation, but rather as a mechanism that supported responsible and sustainable technological development.

A recurring theme throughout the panel was the tendency for governments to prioritize investments in physical digital infrastructure such as broadband networks and data centers while underinvesting in governance mechanisms that ensured these systems operated effectively. Panelists noted that many digital infrastructure initiatives failed not because of technological limitations but because of weak institutional coordination, inadequate policy frameworks, and limited citizen engagement. Without interoperability standards and collaborative governance approaches, digital systems developed by different government agencies became fragmented and inefficient. Moreover, when citizens were not involved in the design and rollout of digital platforms, skepticism undermined adoption.

Key Takeaways from this panel discussion included:

- Digital public infrastructure combines technology, governance frameworks, and institutional accountability mechanisms.
- Digital public goods provided reusable technological tools that enabled scalable digital services.
- Citizens' concerns about digital systems often focused on service effectiveness, data security, and participation in system design.
- Public trust in government institutions significantly influenced the adoption of digital infrastructure initiatives.
- Regulators play a critical role in ensuring innovation evolved alongside data protection safeguards.
- Governance frameworks must keep pace with technological development to prevent fragmentation and mistrust.
- Effective DPI initiatives required co-creation with citizens, strong safeguards, and transparent governance structures



Kwame Owino - Executive Director, Institute of Economic Affairs, Kenya



Karen Bett (Program and Policy Lead, Global Partnership for Sustainable Development Data).



Mark Irura-Moderator

BREAKOUT SESSION 3

Track 1: Data Ownership and Custodianship Data Sovereignty

Title: Promoting Locally Led Awareness on Digital Rights and Data Protection in Western Kenya
led by: ICON Data and Learning Labs Africa

This interactive breakout session led by ICON Data Learning focused on the Ijue Data Yako project—an initiative previously implemented in Kisumu and currently being scaled in Kakamega. The project, supported by Amnesty International, aims to raise awareness on data governance, protection, and responsible use at the grassroots level. The session was delivered in a panel format featuring representatives from Amnesty International, Eagle Wings Organization, and ICON Data Learning. Panelists shared their respective roles and experiences in the design and implementation of the project with Amnesty International highlighting its contribution in providing technical support and capacity building to civil society organizations (CSOs), equipping them with the knowledge and tools necessary to strengthen data governance practices.

Eagle Wings Organization, a participant in the first cohort, demonstrated the practical impact of this support by developing internal data protection policies and cascading acquired knowledge to staff and community members. This underscored the sustainability and multiplier effect of targeted capacity-building interventions. ICON Data Learning emphasized its role in coordinating the project and delivering context-responsive training tailored to grassroots realities. A key issue emerging from the discussion was the limited access to digital infrastructure at the community level, which affects effective data collection, storage, and protection. In addressing this challenge, panelists noted that while much of the data at the grassroots level was still collected manually, data protection could begin with existing systems and practices. Organizations were encouraged to adopt incremental approaches, starting with basic data protection principles and gradually integrating digital tools as capacity improves. Practical solutions shared included the use of accessible platforms such as Google Drive for data storage and management. On impact measurement, Amnesty International indicated that their approach largely focused on qualitative indicators, including changes in attitudes, behaviors, and practices among participating organizations. Examples cited included increased awareness of data privacy rights, adoption of internal data protection policies, and improved data handling practices. It was further noted that the second phase of the project in Kakamega County would build on lessons from the initial implementation, with a focus on strengthening sustainability, contextual adaptation, and scaling impact at the grassroots level.

Key Recommendations

- **Enhance Access to Appropriate Digital Tools:** Stakeholders should invest in affordable and accessible digital infrastructure to support grassroots organizations in improving data management and protection.
- **Institutionalize Continuous Capacity Building:** Ongoing mentorship and follow-up support should complement initial trainings to ensure long-term adoption and integration of data protection practices.
- **Adopt Incremental and Context-Sensitive Approaches:** Data protection initiatives should be designed to align with existing capacities at the grassroots level, allowing organizations to progressively strengthen their systems over time.



From left : Mary Odhiambo (Moderator), Aurelia Miheso - Amnesty International Kenya, Saraphina Ambale - Eagle wings Org, Victor Baraza - ICON Data and Learning Labs



Track 2: Sovereignty and Cross-Border Governance

Title: Data Protection Litigation: Courts, Regulators, and the Future of Data Governance led by: Data Privacy and Governance Society of Kenya

This session examined the increasing importance of litigation in shaping data governance frameworks across East Africa. As digital systems expand and the use of personal data becomes central to governance, commerce, and public services, courts were increasingly being called upon to interpret data protection laws, adjudicate disputes, and define the limits of lawful data use. Legal practitioners, regulators, and civil society representatives reflected on how strategic litigation was emerging as an important tool for protecting privacy rights and strengthening accountability in digital governance.

Speakers noted that the growing number of legal cases related to data protection reflected both the rapid digital transformation occurring in the region and the evolving awareness of citizens regarding their privacy and digital rights. Courts were increasingly being asked to determine whether government institutions and private companies are complying with national data protection laws, constitutional protections, and international human rights standards. Civil society organizations shared experiences of using strategic litigation to challenge unlawful surveillance, misuse of personal data, and opaque digital identity systems. Participants emphasized that litigation had helped clarify legal obligations for both state and non-state actors and had pushed institutions to improve transparency in how personal data was collected, stored, and processed.

Speakers also highlighted the role of data protection authorities and regulatory bodies in supporting judicial processes noting that effective collaboration between regulators and courts was essential for interpreting technical aspects of data protection laws, particularly in cases involving emerging technologies such as biometric identification systems, artificial intelligence tools, and large-scale digital databases.

Participants highlighted several emerging trends:

- Increasing reliance on courts to interpret and clarify national data protection laws and constitutional privacy protections
- Strategic litigation by civil society organizations aimed at safeguarding digital rights and challenging unlawful data practices
- Judicial oversight of government data collection practices, surveillance technologies, and digital identity systems
- Legal disputes involving cross-border data transfers, data localization requirements, and jurisdictional questions in digital governance

The discussion emphasized that judicial institutions played a critical role in ensuring that data governance frameworks were not only adopted but effectively implemented in practice. Courts provided an important avenue for individuals and organizations to seek remedies when data protection rights were violated.

Key recommendations from the session included:

- Strengthening judicial capacity through targeted training on data protection law, digital rights, and emerging technologies
- Enhancing cooperation between courts, data protection authorities, and legal practitioners to ensure consistent interpretation of data governance frameworks
- Promoting regional dialogue and harmonization of legal standards governing cross-border data transfers
- Encouraging public interest and strategic litigation as a mechanism for strengthening accountability in digital governance
- Supporting knowledge exchange among East African legal institutions on evolving jurisprudence related to privacy and data protection

The session concluded that courts and regulatory institutions will play a central role in shaping the future of data governance in East Africa. Strengthening judicial expertise, promoting regulatory collaboration, and ensuring access to legal remedies will be critical to building robust, rights-based data governance systems across the region.

Track 3: Data Infrastructure (Technical Foundations & Systems)

Title: Testing before Scaling: Sandboxes for Data Governance in Digital Public Infrastructure led by: Datasphere Initiative



Risper Onyango-Datasphere initiative, making a presentation on sandboxes



Panelists from right: Brian Beruhanga, Diana Sang, Josephine Kaaniru

This session provided a comprehensive examination of how sandboxes were emerging as a critical tool for the responsible development of Digital Public Infrastructure (DPI). The discussion moved beyond the traditional fintech understanding of sandboxes to explore their application in testing the complex interplay of technology, governance, and trust that underpins DPI layers: digital identity, digital payments, and data exchange. The session began by establishing a common language, defining DPI as a set of shared digital systems built on open standards to enable equitable access to public and private services at a societal scale. Risper Onyango defined a sandbox as a controlled learning environment for structured experimentation, designed to foster multi-actor collaboration and evidence-based decision-making under defined safeguards.

The Datasphere Initiative's research highlights a shift from traditional regulatory sandboxes towards operational and hybrid models, which test not only compliance but also the technical and functional aspects of DPI in real or simulated conditions. The core premise, as illustrated in Risper's presentation, is that trust is the "missing link" in the rapid deployment of technology. Sandboxes are a mechanism to bridge the gap between technological speed and necessary safeguards. They serve to:

- Move collaboration from theory to practice.
- Proactively identify risks and opportunities, such as privacy concerns, surveillance risks, and potential exclusion of vulnerable groups.
- Test both technology and government practices in a contained environment.
- Build trust through demonstrated participation, transparency, and responsiveness.

The Datasphere Initiative's global snapshot of DPI experimentation revealed several key trends:

- Digital Identity is the primary focus of most sandboxes, followed by data exchange and digital payments.
- Successful DPI adoption hinges on trust, which is built through continuous feedback loops and institutional learning. Sandboxes are increasingly being used to test ecosystem readiness and interoperability.
- The AI Nexus: Artificial Intelligence is becoming increasingly embedded within DPI sandboxes, presenting both opportunities and challenges for data governance.

The presentation was followed by a dynamic panel discussion that grounded the research in on-the-ground realities and stakeholder perspectives.

- Diana Sang (Program Manager, Digital Impact Alliance) shared her experience at the nexus of AI and DPI. She noted the massive global investment in AI and emphasized that DPI provided the foundational infrastructure upon which AI can deliver intelligence and efficiency. A primary challenge, she noted, was the difficult transition from policy to practice, citing resource limitations and a lack of clear understanding of what DPI implementation looks like on the ground.

- Brian Beruhanga (Uganda), speaking from a software development and stakeholder perspective, posed a critical question: what does it mean to design a DPI sandbox that is truly in the public interest? He highlighted the frequent lack of Civil Society Organization (CSO) participation. He questioned who gets to define the risks and the values embedded in the technology, and stressed that any experimentation must include conditionality and clear reporting mechanisms if harm occurs.
- Josephine Kaaniru (Research Associate, CIPIT), drawing from research on digital identity in Kenya and Zambia, pointed to the "utility of sandboxing" as a tool for bringing diverse stakeholders together to co-create. She raised concerns about the opacity of government and private sector use of AI and the lack of data sharing. Citing the transition from NHIF to SHA in Kenya, she emphasized that impact assessments are only useful if their findings are made public. Her core reflection was that involving the right people especially affected communities, from the very beginning is essential to developing a comprehensive understanding of risks and ensuring that feedback is genuinely incorporated. The session also addressed the inherent risks and limitations of the sandbox model for DPI development, as outlined in the presentation:
- Stakeholder Engagement: Ensuring meaningful and sustained engagement from all sectors, particularly civil society, remains a significant challenge.
- Opacity and Accountability: Without clear mandates for documentation, monitoring, and auditing, sandboxes can lack transparency.
- Resource Constraints: The pressure for rapid deployment can often overshadow the need for thorough, long-term experimentation.
- Post-Sandbox Governance: A critical gap exists in planning for the "post-sandbox" phase—how learnings are institutionalized and how governance is scaled alongside the technology.

The session concluded with actionable recommendations for strengthening the use of sandboxes in DPI development:

- Clear Mandates for Decision-Making: Government agencies need explicit mandates that link the results of sandbox experimentation to concrete policy and procurement decisions.
- Strengthening Public-Sector Capacity: Investment in DPI must be accompanied by investment in public-sector capacity for cross-disciplinary and cross-stakeholder collaboration.
- Commitment to Continuous Learning: Governments and all ecosystem actors must be equipped with the confidence, skills, and resources to continuously learn, adapt, and iterate based on sandbox outcomes.

Track 4: Ethics, Algorithms, and Accountability

Title: Bridging the Gap: A Subnational Dialogue on Collaborative Data Governance for Equitable Development in Kenya's Counties led by: Kenya National Bureau of Statistics (KNBS) and CSOs



Panelists

- Harriet Atieno – Homa Bay County Government
- Wilfred Kazungu – Kilifi County Government
- Sara Mwikali – Kenya National Bureau of Statistics (KNBS)
- Tobias Onyango – Kisumu County
- Charles Njenga – Mombasa County / Civil Society
- Albert Nmutu – Nandi County



This session was moderated by Christine Ajulu and Benjamin Charagu from Open Institute. The breakout session focused on the growing importance of collaborative data governance at the subnational level, particularly in the context of Kenya's devolved governance system. The discussion explored how county governments, national statistical agencies, and civil society organizations can work together to improve the collection, validation, and use of data to support equitable development outcomes. A key premise underlying the session was that although significant volumes of data were collected by governments, civil society organizations, and research institutions, these datasets often remained fragmented, underutilized, or disconnected from decision-making processes. The session therefore examined the barriers that prevented effective collaboration between stakeholders and identified opportunities for building stronger partnerships that ensured data contributed meaningfully to development planning.

The panel brought together representatives from several county governments, the Kenya National Bureau of Statistics, and civil society organizations. The discussion emphasized that subnational governments play a critical role in translating national development policies into localized planning frameworks. However, many counties continue to face challenges in accessing reliable, disaggregated, and timely data necessary for evidence-based planning. At the same time, civil society organizations and research institutions frequently generated valuable datasets that could inform county development strategies but are rarely integrated into official planning systems. This disconnect formed the central theme of the discussion. One of the key issues highlighted during the discussion was the difficulty county governments face in integrating civil society-generated data into formal planning processes. Harriet Atieno of Homa Bay County explained that while civil society organizations collect important datasets on issues such as health, gender equality, agriculture, and climate change, these datasets were often not utilized in county planning due to concerns about data reliability, relevance, and ownership. For planners working within government institutions, using data that is not officially produced by the state raised questions about accountability and credibility. County planners must be able to defend the data they use in policy formulation and budget allocation processes, and therefore require assurance that external datasets meet accepted standards of quality and validity.

Atieno noted that another challenge lies in the level of disaggregation required for county planning. Development planning at the subnational level often required highly localized data, sometimes down to ward or village levels. Civil society data may not always be collected using the same geographical or statistical frameworks used by government planning departments, making it difficult to integrate into official planning systems. As a result, even when useful data exists outside government institutions, structural barriers prevent its effective use.

Wilfred Kazungu from Kilifi County offered insights into how data collaboration has been evolving within the health sector. He explained that health departments within county governments had relatively structured systems for collecting data through standardized national tools used by health facilities and community health workers. These systems enabled counties to monitor health indicators and track the performance of programs such as immunization campaigns. However, Kazungu noted that significant amounts of valuable data was also collected by external actors, including research institutions and non-governmental organizations. For example, institutions such as the KEMRI-Wellcome Trust research program collected extensive health and demographic surveillance data that could complement government datasets. Historically, however, collaboration between these institutions and county governments has been limited due to concerns about data ownership and sharing protocols. Kazungu highlighted a recent shift toward greater collaboration, where research institutions and county governments are beginning to share anonymized datasets to improve planning processes. Such collaborations are particularly important when counties attempt to calculate accurate denominators for public health indicators such as immunization coverage. Without reliable population data, counties may struggle to set realistic targets and evaluate program performance effectively.

Sara Mwikali of the Kenya National Bureau of Statistics (KNBS) emphasized the role of the national statistics agency in coordinating data systems across both national and county levels. KNBS is mandated to collect, process, analyze, and disseminate official statistics for the country, and it plays a critical role in ensuring the standardization and quality of data used for policymaking. Mwikali explained that KNBS works closely with county governments to produce county statistical abstracts, which compile key indicators across sectors such as health, education, population, and economic development.



A major focus of KNBS's work has been the integration of citizen-generated data, which refers to datasets collected by civil society organizations or communities themselves. Mwikali noted that this approach helps address data gaps and reduces duplication in data collection efforts. Instead of repeatedly surveying the same communities, KNBS can validate and incorporate data collected by civil society organizations, provided that the datasets meet established quality standards. To ensure credibility, KNBS has developed frameworks such as CASECOV, which assess the quality of external datasets based on criteria such as methodology, timeliness, and relevance. Through these mechanisms, civil society data can be evaluated and potentially incorporated into official statistics, thereby strengthening collaboration between state and non-state actors.

The discussion also highlighted tensions between government and civil society actors regarding the use of data. Tobias Onyango of Kisumu County emphasized that civil society organizations often generated data that reflected the realities faced by communities on the ground. These datasets may capture issues that government systems fail to document adequately, such as community health challenges or gaps in service delivery. However, Onyango observed that civil society data is sometimes viewed with skepticism by government institutions, particularly when it highlights governance failures or contradicts official statistics. At the same time, communities themselves may trust civil society organizations more than government institutions when sharing sensitive information, particularly in areas such as health and social services. This dynamic creates a complex relationship between government and civil society actors. While civil society organizations often seek to complement government efforts, differences in institutional incentives and accountability structures created tensions that hindered effective collaboration.

Christine Ajulu of the Open Institute emphasized the need to build stronger data ecosystems that connect government institutions, civil society organizations, and communities. She highlighted initiatives such as civil society data fellowships that aimed at strengthening data management and governance capacities within civil society organizations. By equipping civil society actors with skills in data protection, analysis, and ethical data management, these programs helped to ensure that community-generated data can be used responsibly and effectively in policymaking processes. The session emphasized that collaborative data governance required more than simply sharing datasets; it required building trust between institutions, developing standardized methodologies, and creating platforms where stakeholders can regularly exchange information and insights. Without these mechanisms, data systems risk remained fragmented, reducing their potential impact on development planning.

Key Takeaways

- Collaboration between county governments, national statistical agencies, and civil society organizations is essential for strengthening data governance at the subnational level.
- Many counties struggle to integrate civil society data into planning processes due to concerns about credibility, ownership, and methodological differences.
- Research institutions and civil society organizations generate valuable datasets that can complement government data, particularly in sectors such as health and community development.
- The Kenya National Bureau of Statistics plays a crucial coordinating role in validating and integrating citizen-generated data into official statistics.
- Civil society organizations often have greater trust among communities, enabling them to collect data that may not be captured by government systems.
- Strengthening collaborative data ecosystems requires shared standards, data validation frameworks, and continuous dialogue between stakeholders.

Track 4: Ethics, Algorithms, and Accountability

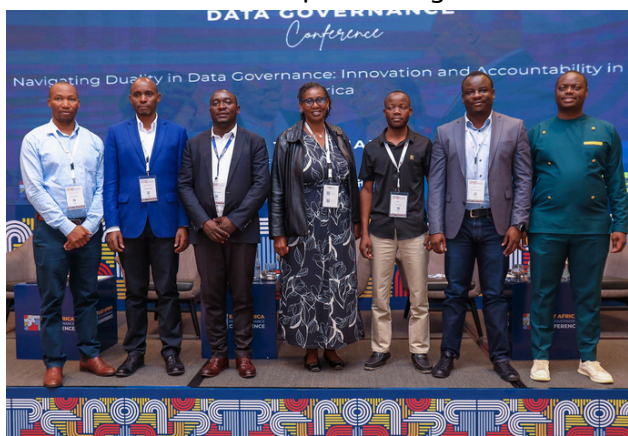
Title: Privacy-Enhancing Frameworks and Technologies led by: African Population and Health Research Center (APHRC)

This breakout session explored emerging technological and governance approaches designed to strengthen privacy protection in an increasingly data-driven digital environment. Participants examined how Privacy-Enhancing Technologies (PETs) can help organizations collect, process, and share data responsibly while reducing the risks associated with exposing sensitive personal information.

Speakers who led the conversation included experts from African Population and Health Research Center (APHRC) i.e. Boniface, Wanjiru Mwangi-Research Officer, Sirus-scientist, Nelson -data officer who emphasized that as governments, research institutions, and private sector organizations expand their use of digital systems, there is growing pressure to balance the value of data-driven innovation with the need to safeguard individual privacy and data rights. Privacy-enhancing frameworks and technologies were highlighted as practical tools that enable this balance by allowing data to be analyzed or shared in ways that limit direct exposure of personally identifiable information. Participants discussed how PETs can play a crucial role in sectors such as health research, financial services, public administration, and social protection programs, where large volumes of sensitive data are routinely collected and processed. In particular, health and research institutions were identified as key beneficiaries of privacy-preserving technologies, as they often require access to aggregated data for policy analysis and research while maintaining strict confidentiality standards. The session also highlighted the importance of embedding privacy safeguards into digital systems at the design stage rather than attempting to add them after systems have already been deployed. Participants noted that integrating privacy considerations early in the development process can significantly reduce risks related to data breaches, misuse, and unauthorized access.

Technologies and approaches highlighted during the session included:

- Data anonymization and pseudonymization tools that remove or mask identifying information while allowing datasets to remain useful for analysis
- Secure data sharing protocols that enable institutions to exchange data while maintaining strict access controls and accountability mechanisms
- Advanced encryption systems designed to protect data both in storage and during transmission across digital networks
- Federated learning models, which allow machine learning systems to analyze distributed datasets without requiring sensitive information to be centralized in a single database
- Differential privacy techniques, which add statistical noise to datasets to prevent identification of individuals while preserving overall data utility.



Participants emphasized that while these technologies offered significant promise, their successful implementation depended on supportive governance frameworks and institutional capacity. Many organizations across East Africa still faced challenges related to limited technical expertise, inadequate digital infrastructure, and insufficient regulatory guidance on the adoption of privacy-preserving technologies. The discussion further highlighted the importance of aligning technological innovation with national and regional data protection

frameworks. Participants called for stronger collaboration between policymakers, technology developers, research institutions, and civil society organizations to promote responsible innovation and ensure that privacy-enhancing tools are adopted in ways that support human rights and ethical data use.

Key reflections from the session included:

- The need for increased capacity-building and technical training for institutions adopting privacy-enhancing technologies
- The importance of clear regulatory frameworks that provide guidance on responsible implementation of PETs
- Encouraging public-private partnerships to support innovation and investment in privacy-preserving infrastructure
- Integrating privacy-by-design and privacy-by-default principles into digital system development and procurement processes.

The session concluded that privacy-enhancing technologies represent an important pathway toward building trustworthy and resilient digital ecosystems in East Africa. However, their effectiveness will depend on sustained investment in technical capacity, supportive policy frameworks, and cross-sector collaboration to ensure that privacy protection remains a core pillar of digital transformation efforts across the region.

Track 5: Economics & Value of Data (Monetization & Shared Benefit)

Title: Cross-Border & Regional Governance: Interoperability Is Political, Not Technical

Panelists

- Ryan Maninga – United Nations Environment Programme (UNEP)
- Michael Michie – Founder & CEO, Everse Tech
- Georgina Giathi – Advocate and Data Governance Legal Expert
- Jessica Wangai-Sintal Africa

This breakout session explored the political, institutional, and governance dimensions of cross-border data sharing and regional interoperability in East Africa. Moderated by Jessica Wangai of Sintal Africa, the discussion examined the growing recognition that challenges surrounding data interoperability are not purely technical but deeply embedded in political, institutional, and governance structures.

The panel brought together experts from environmental data governance, legal practice, and digital infrastructure development to explore how regional collaboration frameworks can enable more effective use of data for shared public goods such as disaster response, environmental monitoring, and regional development. The conversation began with the observation that discussions about data interoperability often focus on technical challenges such as incompatible data systems, fragmented data formats, and infrastructure limitations. However, the panel emphasized that these issues represent only a small portion of the broader challenge. Even where technical solutions existed, institutional reluctance, legal uncertainties, and concerns about sovereignty frequently prevent data from being shared across organizations and borders. As such, the panel framed interoperability as fundamentally a governance challenge that requires trust, shared norms, and political commitment across institutions and countries.

Ryan Maninga provided a case study based on work conducted with the United Nations Environment Programme (UNEP) on transboundary data sharing across Kenya, Uganda, and Tanzania. The project sought to examine how environmental and disaster-related data flows across national borders and to identify the barriers that prevent effective regional data sharing. The study was particularly focused on disaster preparedness, where timely data sharing can significantly improve the ability of governments and humanitarian agencies to respond to emergencies. Maninga explained that disasters such as floods, droughts, and disease outbreaks rarely respect national borders. For example, flooding along shared river basins can simultaneously affect communities across multiple countries.



From left: Ryan Maninga, Michael Michie, Georgina Giathi, Jessica Wangai



Effective response mechanisms therefore depend on the ability of institutions to share data quickly and coordinate interventions across jurisdictions. However, the project revealed that many institutions continue to operate within isolated data environments, where datasets are treated as proprietary assets rather than shared resources. Another major challenge identified was the lack of standardized data formats. Many institutions still store data in non-interoperable formats such as static reports or PDF documents, which cannot easily be integrated into digital systems for analysis and innovation. This limits the ability of researchers, innovators, and humanitarian organizations to develop early warning systems and predictive tools that rely on real-time data flows. Maninga also noted that misunderstandings about data protection laws often contribute to institutional reluctance to share information. In many cases, organizations avoid sharing data altogether because of uncertainty about legal requirements, even when the data involved is not sensitive personal data. This highlights the need for improved institutional capacity and clearer regulatory guidance on what types of data can be shared for public interest purposes.

Michael Michie brought a technological perspective to the discussion, drawing on his experience building digital infrastructure and deploying high-performance computing systems in the region. While acknowledging that technical interoperability challenges do exist, Michie emphasized that many of the barriers to data sharing are rooted in geopolitical and policy considerations rather than technological limitations. He pointed out that access to advanced computing infrastructure, including AI hardware and specialized chips, is often influenced by international trade restrictions and geopolitical policies. These restrictions can limit the ability of countries in the Global South to develop their own data ecosystems and technological infrastructure. As a result, digital innovation ecosystems in many African countries remain dependent on external technology providers and regulatory frameworks. Michie also highlighted the importance of legal and governance safeguards when sharing data across institutions and countries. Even where technical systems such as APIs can facilitate data exchange, organizations must still address legal questions related to data protection, encryption standards, anonymization, and access rights. These governance mechanisms are necessary to ensure that shared data is used responsibly and that the rights of individuals and institutions are protected.

Georgina Giathi provided a legal analysis of why interoperability challenges often manifested as political rather than technical problems. She explained that data was increasingly viewed as a form of property or strategic resource, which naturally led institutions and governments to adopt protective approaches to its management. Just as individuals protected their physical property, governments and organizations tended to guard their data assets closely. Giathi illustrated this concept using the analogy of a private home: even when access routes exist that allow others to pass nearby, property owners still feel compelled to erect boundaries and control access points. Similarly, organizations that control valuable datasets often establish barriers to sharing, even when broader collaboration could generate collective benefits. From a governance perspective, the challenge therefore becomes how to design systems that allow data to be shared while still preserving sovereignty and control. Legal frameworks such as data-sharing agreements, memoranda of understanding, and purpose-limited access arrangements can provide mechanisms for balancing these interests. However, these arrangements required institutional trust and political commitment, which are often more difficult to establish than technical infrastructure.

A recurring theme throughout the discussion was the importance of designing governance models that preserved institutional control while enabling collaboration. One approach highlighted during the session was the concept of federated data systems, where data remains under the control of the original data producer but can be accessed through standardized interfaces such as APIs. In such systems, organizations need not transfer ownership of their data to a central repository. Instead, they can allow controlled access to specific datasets for defined purposes, such as environmental monitoring or disaster response. This approach will help address concerns related to sovereignty and ownership while still enabling innovators and researchers to build solutions that rely on shared data ecosystems. Panelists noted that federated data architectures could be particularly valuable in addressing regional challenges such as climate change, environmental degradation, and public health emergencies, where coordinated data sharing across countries is essential.

Participants also discussed the institutional incentives that shape data sharing behavior. In many organizations, data is treated as a strategic asset that provides competitive or institutional advantage. As a result, institutions may be reluctant to share data unless clear value propositions exist. Audience contributions highlighted that demonstrating the practical benefits of data sharing can play a critical role in overcoming institutional resistance. When organizations see tangible outcomes such as improved disaster response systems, better service delivery, or enhanced research capacity they may become more willing to collaborate. Another key issue raised during the discussion was the concept of data monetization and shared benefit. Participants questioned how value generated from data-driven innovations can be equitably distributed, particularly when private sector organizations profit from datasets originally generated by public institutions or communities.

Key Takeaways

- Data interoperability challenges are primarily political and governance-related rather than purely technical.
- Cross-border issues such as disaster response and environmental monitoring require stronger regional data-sharing frameworks.
- Institutional reluctance to share data is often driven by concerns about sovereignty, ownership, and legal liability.
- Technical solutions such as APIs and federated data systems can enable controlled data sharing without transferring ownership.
- Misinterpretation of data protection laws frequently leads organizations to avoid sharing even non-sensitive data.
- Building trust among institutions and demonstrating the practical value of data collaboration are essential for advancing regional interoperability.

LIGHTNING TALKS

Track 3: Data Infrastructure (Technical Foundations & Systems)

Title: How structured data collection and governed dashboards can advance accountability in East Africa's digital transformation presented by John Muccheke- Open Institute



This presentation focused on the critical role that structured data systems and governed digital infrastructure played in strengthening accountability within East Africa's rapidly evolving digital ecosystem. The presenter emphasized that while the region had made significant strides in adopting digital technologies and data-driven systems, the pace of innovation must be matched by strong governance mechanisms that ensured reliability, transparency, and responsible use of data. The presentation began by highlighting what Mr. Muccheke

described as the core challenge in East Africa's digital transformation: balancing the promise of rapid innovation with the risks that arise when digital infrastructure evolves faster than governance frameworks. As digital technologies expanded across sectors such as health, finance, public administration, and civic participation, the absence of clear rules and accountable systems could undermine trust and create vulnerabilities within digital ecosystems. He explained that the region's digital transformation presented both significant opportunities and serious governance risks. On one hand, data-driven systems enable innovations such as mobile financial services, remote health services, and citizen-generated data platforms that can improve public service delivery and expanded economic participation. On the other hand, the rapid adoption of digital technologies raises critical concerns around privacy protection, data sovereignty, algorithmic accountability, and institutional oversight.



A key message from the presentation was that innovation and accountability must evolve together. To address this challenge, the speaker proposed the development of governed infrastructure frameworks that integrated technical systems with policy and oversight mechanisms. The concept of a governed infrastructure framework was presented as a central component of responsible digital transformation. Such frameworks would ensure that digital systems are designed with safeguards that promote privacy protection, transparency, accountability, and compliance with regulatory standards. The presentation highlighted several governance pillars that should be embedded within digital infrastructure systems across the region:

- Privacy protections and security mechanisms to safeguard personal data and build public trust in digital systems.
- Data sovereignty considerations to ensure that countries maintain control over critical national data assets and digital infrastructure.
- Ethical algorithmic oversight to address potential biases and risks associated with automated decision-making systems.
- Transparent governance mechanisms that allow institutions and citizens to understand how data is collected, processed, and used.

The presentation also explored the technical challenges that arose in data governance once data had been collected and began moving across multiple systems and platforms. The speaker illustrated how data could lose its integrity as it travelled across different tools, formats, and processing environments. As datasets moved through systems, they may be cleaned, transformed, or reinterpreted by analysts, often leading to loss of metadata, shifts in definitions, and reduced traceability. This process ultimately results in situations where decision-makers rely on data that is incomplete, unverifiable, or disconnected from its original context. The speaker described this phenomenon as similar to a “game of telephone,” where information gradually changed as it passed through multiple intermediaries. By the time data reaches policy-makers or institutional leaders, it may no longer accurately represent the original information collected in the field. The presentation stressed that this issue is not primarily a technological failure but a governance failure.

Without clear systems for maintaining data lineage, metadata integrity, and standardized data governance practices, even sophisticated digital tools can produce unreliable outcomes. To address these challenges, the presentation introduced a technical approach centered on structured data collection systems and governed dashboards. The speaker demonstrated how controlled data pipelines can improve accountability by ensuring that information collected in the field remains consistent, verifiable, and traceable throughout its lifecycle. One example presented during the session was a system known as Sabasi, which was developed as a structured data collection and visualization platform designed specifically for African operational environments. The Sabasi system replaces ad-hoc data collection processes with a secure and governed pipeline for managing primary field data.

The system operates across two key components:

- Sabasi Survey (Acquisition Layer): This component functions as the primary data collection interface, allowing field teams to capture structured information through mobile devices. The system supports features such as offline data collection, schema enforcement, and standardized data capture formats, ensuring that field data remains consistent and reliable even in environments with limited connectivity.
- Sabasi Dashboard (Presentation Layer): The dashboard component transforms structured datasets into interactive visualization tools that support decision-making. It integrates processes such as data ingestion, widget rendering, and decision-support modeling, enabling policymakers and analysts to interpret data in ways that are transparent and actionable.

Combining these two layers created a governed data pipeline in the system that connected field-level data collection directly to institutional decision-making processes. This structure reduces the risk of data distortion and improves accountability by maintaining a clear link between the original source of information and the final outputs used in policy discussions.

Mr. Mucheke emphasized that such systems were particularly important for public sector governance and development programs, where data often informed decisions on resource allocation, public services, and development interventions. Without reliable data systems, governments and institutions struggle to make evidence-based decisions or evaluate the impact of their programs. The presentation concluded by emphasizing that strong technical infrastructure must be accompanied by strong governance frameworks. Building digital tools alone was not sufficient; institutions must also invest in systems that maintain data integrity, support transparency, and enable responsible decision-making. Ultimately, the speaker argued that structured data systems can serve as a foundation for accountability in digital governance, helping governments, civil society organizations, and development actors ensure that digital transformation leads to measurable and equitable outcomes across East Africa.

Track 3: Data Infrastructure (Technical Foundations & Systems)

Title: ORPP'S Journey in Political Data Governance: Navigating Innovation and Accountability

Presenter: Joshat Nyongesa-Office of the Registrar of Political Parties-ORPP

This presentation explored the evolving role of the Office of the Registrar of Political Parties (ORPP) in strengthening political data governance in Kenya. The presentation highlighted how digital systems and governance frameworks are being leveraged to enhance accountability, transparency, and efficiency in the management of political party records. Mr. Nyongesa emphasized that as democratic processes increasingly rely on digital systems, ensuring the integrity, security, and reliability of political data becomes essential for maintaining public trust and safeguarding democratic institutions. The presentation began by outlining the constitutional and institutional foundations guiding the operations of the ORPP.



The Constitution of Kenya (2010) entrenches multiparty democracy and guarantees political rights under Article 38, including the right of citizens to form, join, and participate in political parties. The Constitution further envisions political parties that adhere to democratic principles and maintain a national character as stipulated under Article 91. Within this framework, the Political Parties Act established the ORPP and mandated it to regulate and register political parties as well as administer the Political Parties Fund. These responsibilities require the management of significant volumes of political and personal data, including party membership records, compliance reports, and financial disclosures. Mr. Nyongesa further discussed the legal and regulatory framework supporting political data governance in Kenya. Several key legislative and policy instruments guide the processing, management, and protection of political data. These include:

1. Data Protection Act (2019) – regulates the processing of personal data and establishes safeguards for data privacy.
2. Access to Information Act (2016) – guarantees citizens the right to access information held by public institutions.
3. Computer Misuse and Cybercrimes Act (2018) – addresses cybercrime and strengthens digital security frameworks.
4. National ICT Policy (2019) – provides the policy framework for the development and governance of ICT systems in Kenya.
5. Kenya Artificial Intelligence Strategy (2025–2030) – aims to ensure that emerging AI ecosystems remain secure, ethical, and accountable.



Within this regulatory environment, data governance within ORPP played a critical role in ensuring the integrity and security of political party information. He emphasized that the office managed sensitive datasets related to political party membership, regulatory compliance, and financial records. Effective data governance was therefore necessary to maintain accurate records, ensure accountability, and support regulatory oversight of political parties. A central focus of the presentation was the Integrated Political Parties Management System (IPPMS), which served as the primary digital platform for managing political party records. The system was developed to enhance efficiency, transparency, and accountability in the registration and management of political party data. Developed in 2017 and rolled out in 2018, IPPMS functions as a web-based application designed to streamline the collection, verification, and management of political party membership data.

Key features of the IPPMS platform include:

- Self-registration and password reset functionalities for users.
- Integration with the Integrated Population Registration System (IPRS) for identity verification.
- Integration with Mobile Network Operators (MNOs) to facilitate communication and verification processes.
- Integration with the eCitizen platform to support digital public service delivery.
- Enhanced user control mechanisms to improve data management and oversight.
- Integration with the Independent Electoral and Boundaries Commission (IEBC) voter register and National Council for Persons with Disabilities (NCPWD) databases to improve accuracy and inclusivity in political party membership data.

The system also incorporates *USSD-based access (509#) to expand accessibility for citizens who may not have access to internet-enabled devices. Through this platform, citizens are able to:

- Check their political party membership status.
- Join or resign from a political party.
- Provide consent or object to a political party registration using SMS verification mechanisms.

This approach was highlighted as an important step toward enhancing public participation and digital inclusion, particularly for individuals in rural or underserved areas. The presentation also provided insights into the scale of political party membership data managed by the ORPP. According to the data shared, the political party membership database contained over 23 million registered members, with approximately 18 million registered voters and over 5.6 million non-voters. This demonstrates the significant size and complexity of political data systems managed by the institution. Despite these technological advancements, the presentation identified several emerging concerns in political data governance, including:

- Registration of individuals into political parties without their consent.
- Duplicate or inaccurate membership records across party databases.
- Potential misuse of personal data.
- Weak data governance practices within some political party systems.

These challenges have broader implications for democratic governance and public confidence in political institutions. The speaker noted that weaknesses in political data management led to:

1. Erosion of public trust in political institutions.
2. Compromised internal party democracy.
3. Increased risks of personal data exposure.
4. Questions regarding the integrity and credibility of political party membership registers.

To address these concerns, the presentation emphasized the importance of public empowerment and awareness. Citizens must be provided with accessible mechanisms to verify their political party membership status and exercise their rights. Strengthening transparency and accountability in membership registration processes is also critical to maintaining public trust. In concluding the presentation, the speaker reaffirmed the commitment of the ORPP to strengthening political data governance systems. The institution intends to continue enhancing digital infrastructure, strengthening policies and partnerships, and improving safeguards for personal data protection. These efforts aim to ensure secure and accountable political party membership management while reinforcing public confidence in Kenya's democratic institutions.



BREAKOUT SESSION 4

Track 2: Sovereignty and Cross-Border Governance

Title: Governance in Practice: Building Integrated, Sovereign, and Accountable Data & AI Systems in Africa

Lead Organization: (CIPIT), Strathmore University, Shapers Youth Network, ICTLC- ICT Legal Consulting International

Panelists

Florence Ogonjo – AI Policy Researcher, CIPIT – Strathmore University

Moses Awambwa – Multimedia Journalist & Development Communication Researcher

Alfred Nyaga – Founder, Digital Ethics Hub.

This breakout session examined the complex governance challenges arising from the rapid adoption of artificial intelligence and digital data systems across Africa. The panel discussion focused particularly on how governments can design integrated governance frameworks that balanced innovation, sovereignty, and accountability while protecting citizens' rights. Moderated by Wendy Kuio, the conversation brought together experts in AI governance, digital rights, and development communication to reflect on how emerging technologies were reshaping public administration, economic systems, and social structures across the continent. The session began by acknowledging that artificial intelligence was increasingly embedded in critical public sector systems, including national identity infrastructure, education placement systems, healthcare technologies, and digital public services. While these technologies offered significant opportunities for improving efficiency and expanding service delivery, they also raised profound governance questions about accountability, transparency, and the protection of fundamental rights. Panelists therefore explored how African countries could design governance models that allowed innovation to flourish while ensuring that technological systems remained ethical, inclusive, and aligned with democratic values.

A central theme throughout the discussion was the need to move beyond fragmented governance approaches toward integrated frameworks that link data governance, AI governance, and digital sovereignty strategies. Panelists emphasized that many African countries were still in the early stages of developing AI regulatory systems, which presents both challenges and opportunities. On the one hand, the rapid pace of technological change risked outpacing regulatory capacity. On the other hand, the relative novelty of AI adoption in Africa provided governments with a valuable opportunity to design governance frameworks that are tailored to local contexts rather than simply replicating regulatory models from other regions.

Integrating Data Governance and AI Regulation

Florence Ogonjo highlighted that the development of data protection laws across Africa provided an important foundation for future AI governance frameworks. Because AI systems rely heavily on data as their core resource, the legal frameworks governing data collection, processing, and protection inevitably shape how AI technologies operate. According to Okonjo, the emergence of data protection legislation before AI-specific regulations should not necessarily be viewed as a regulatory gap but rather as an opportunity to build coherent governance frameworks that address both data and algorithmic systems simultaneously. She explained that many existing legal instruments including consumer protection laws, intellectual property frameworks, and digital rights policies can already be interpreted in ways that address aspects of AI governance. These frameworks may not have been designed specifically with AI in mind, but they still provide important safeguards that can guide the responsible deployment of emerging technologies. The challenge therefore lies in ensuring that policymakers understand how these legal frameworks intersect and how they can be adapted to regulate AI systems effectively.



Ogonjo also emphasized that African countries should avoid the temptation to simply replicate foreign regulatory models without considering local contexts. Instead, governments should take advantage of the current policy window to study the specific ways in which AI is being deployed in their societies and design governance frameworks that respond to locally observed risks and harms. By learning from both global experiences and domestic case studies, policymakers can develop regulatory approaches that are both innovative and contextually appropriate.

The Digital Divide and Exclusion of Rural Communities

Moses Awambwa shifted the conversation toward the societal impacts of digital transformation, particularly the persistent inequalities between urban and rural communities. Drawing on research into digital governance and development communication, he argued that rural populations often remained excluded from the benefits of the digital economy due to infrastructure limitations and policy neglect. He highlighted the stark contrast between urban areas, where access to digital infrastructure such as electricity and internet connectivity was relatively widespread, and rural regions where these resources remain scarce. While urban populations increasingly benefited from digital services and technological innovation, many rural communities struggled to access even basic communication infrastructure. He noted that this digital divide had significant implications for the adoption of AI and digital public services. If governments continue to digitize services without addressing underlying infrastructure gaps, a large proportion of the population may be excluded from accessing essential services. For example, in some rural areas communities must travel long distances simply to access internet connectivity or mobile network coverage. These disparities highlight the need for governance frameworks that prioritize inclusive infrastructure development alongside technological innovation. Awambwa also pointed to recent government initiatives aimed at expanding digital access, including proposals to establish ICT hubs in wards across the country. While such initiatives hold promise for bridging the rural-urban digital divide, their success will depend on sustained investments in infrastructure, connectivity, and digital literacy.

Ethical Design and Responsible AI Development

Alfred Nyaga expanded the discussion by focusing on the ethical challenges associated with AI systems and the importance of embedding ethical safeguards into technological design processes. He emphasized that AI governance should not be limited to regulatory compliance but should also involve proactive ethical design choices that address potential risks before systems are deployed.

Nyaga described artificial intelligence as essentially “data in motion,” highlighting how algorithmic systems rely on continuous flows of data to learn and make decisions. Because these systems operated at scale, they had the potential to amplify existing inequalities and biases within society. Marginalized communities, including rural populations and vulnerable groups, therefore face disproportionate harms if AI systems were deployed without adequate safeguards. To mitigate these risks, Nyaga argued that developers and policymakers adopt design principles such as privacy-by-design and ethics-by-design, ensuring that ethical considerations were integrated into technological architecture from the outset rather than being addressed only after systems are deployed. He also stressed the importance of strengthening legal frameworks that govern emerging technologies to ensure that AI systems are deployed responsibly and transparently.

Digital Sovereignty and Foreign Cloud Infrastructure

Another key topic addressed during the session was the issue of digital sovereignty, particularly in relation to the increasing reliance on foreign cloud service providers and external digital infrastructure. Panelists noted that many African governments stored critical public sector data on cloud platforms operated by multinational technology companies, raising questions about control, jurisdiction, and long-term technological dependency.

Awambwa explained that global cloud infrastructure was heavily concentrated in a small number of countries, with a significant proportion of the world's data centers located in the United States. This concentration of digital infrastructure meant that data generated within African countries was often stored and processed under foreign legal regimes. Such arrangements can create vulnerabilities, particularly in situations where geopolitical conflicts, regulatory disputes, or technological disruptions affect access to these systems. The discussion also highlighted examples where disruptions to digital infrastructure such as damaged submarine cables or cyberattacks have resulted in widespread service interruptions. These incidents illustrate the risks associated with heavy reliance on external digital infrastructure for critical public services.

Policy Implementation and Regulatory Gaps

Florence Okonjo concluded the discussion by reflecting on the gap between policy development and policy implementation in digital governance. While many African countries had developed comprehensive legal frameworks addressing data protection and digital governance, the effectiveness of these frameworks often depended on their practical implementation. She pointed out that Kenya's Data Protection Act and related regulatory guidelines already included provisions governing issues such as cross-border data transfers and cloud computing. However, challenges frequently arose when organizations failed to implement these safeguards effectively or when regulatory oversight mechanisms lacked sufficient capacity to enforce compliance. Okonjo argued that strengthening institutional capacity, improving transparency in data governance practices, and ensuring accountability mechanisms were essential for translating legal frameworks into meaningful protections for citizens.

Key Takeaways

- Integrated governance frameworks are essential for managing the intersection of data governance, AI governance, and digital sovereignty.
- Existing legal frameworks including data protection, consumer protection, and intellectual property laws—can provide foundations for AI regulation.
- African policymakers should avoid simply replicating foreign AI regulatory models and instead design frameworks that respond to local contexts.
- The rural–urban digital divide remains a major barrier to inclusive participation in the digital economy.
- Ethical AI governance requires embedding safeguards such as privacy-by-design and ethics-by-design into technological systems.
- Reliance on foreign cloud infrastructure raises concerns about digital sovereignty and long-term technological dependency.



Wendy Kuio – ICT Legal Consulting International (ICTLC); Alfred Nyaga – Founder, Digital Ethics Hub; Moses Awambwa – Multimedia Journalist & Development Communication Researcher; Florence Ogonjo-AI policy

Track 4: Ethics, Algorithms, and Accountability

Title: Voices from the Ground: A People-Centered Dialogue on Ethics, Evidence, and Safety in East Africa's Data Ecosystem: Story Zangu Hub, Rural Women in Street Health



From left to right: Josephine Achieng, Hassan Kibwana, Abigael Wakarima, Belinda Nabwire, Annet Opiyo

This participatory session centered on amplifying community voices within the broader discourse on data governance in East Africa. Unlike many technical or policy-oriented discussions, the session created a space for grassroots organizations. Unlike many technical or policy-oriented discussions, the session created a space for grassroots organizations, community advocates, and researchers to share lived experiences from communities directly affected by digital technologies and data systems. Participants emphasized that data governance conversations often take place within regulatory, legal, or technical arenas, leaving out the perspectives of citizens whose data is routinely collected, processed, and analyzed by governments, private companies, and development actors. This disconnect could result in policies and digital systems that failed to account for the social realities, vulnerabilities, and priorities of the communities they intended to serve. Community representatives shared examples of how digital platforms, biometric registration systems, mobile health programs, and social protection databases increasingly shape people's access to services and opportunities. While these systems can improve efficiency and service delivery, participants noted that they can also introduce new risks particularly for marginalized populations such as informal workers, women, youth, and persons living in underserved urban and rural areas. The dialogue highlighted how limited awareness of digital rights often prevented individuals from understanding how their personal data is collected, shared, or used. Many citizens remain unaware of the existence of data protection laws, complaint mechanisms, or regulatory bodies that are meant to safeguard their rights. As a result, individuals may not have the knowledge or confidence to question how institutions handled their data. Participants also discussed the ethical challenges associated with data collection practices in research and development programs. Community representatives called for more transparent and accountable processes when collecting community data, including clear communication about consent, data ownership, and how collected information will ultimately be used.

Key issues raised during the discussion included:

- Limited public awareness and understanding of data protection rights and responsibilities
- Lack of meaningful participation by citizens and community groups in the design of digital policies and data governance frameworks
- Risks faced by marginalized communities within digital systems, including exclusion, profiling, or misuse of sensitive information
- Insufficient mechanisms to ensure that community perspectives inform technology design and deployment

Participants stressed that ethical data governance cannot be achieved solely through regulatory compliance or technical safeguards. Instead, it must be grounded in inclusive processes that recognize communities as active stakeholders rather than passive data sources.

Key recommendations emerging from the session included:

- Expanding digital literacy initiatives to help communities understand their rights, risks, and responsibilities within digital ecosystems
- Creating public engagement platforms that enable citizens to meaningfully participate in digital policy and data governance discussions
- Strengthening partnerships between civil society organizations, community networks, and policymakers to ensure inclusive policy development
- Promoting community-led research and evidence generation to better inform ethical data governance practices
- Encouraging institutions to adopt participatory and human-centred approaches when designing data systems and digital services.

The session concluded that building ethical and accountable data ecosystems in East Africa required placing people and communities at the center of governance processes. Participants emphasized that inclusive dialogue, transparency, and sustained investment in public awareness would be essential to ensuring that digital transformation advances equity, safety, and trust for all members of society



Track 4: Ethics, Algorithms, and Accountability

Title: Human-in-the-loop verification with AI during emergencies like elections

Led by Linda Ngari, a media representative, this session examined the growing role of Artificial Intelligence (AI) in shaping information ecosystems, particularly during high-risk periods such as elections and public emergencies. Discussions emphasized the importance of human oversight in AI-driven information systems



noting that while AI tools can significantly enhance content monitoring and verification, they are not sufficiently reliable without human review. A central theme of the session was the concept of “human-in-the-loop” verification, which ensures that AI-generated outputs are reviewed and interpreted by people before being acted upon or disseminated. Participants noted that AI systems often struggle with contextual interpretation, bias detection, and linguistic nuance, especially in regions where local languages and cultural contexts are underrepresented in training datasets.



The discussion also highlighted the growing threat of AI-generated misinformation, including deepfakes and manipulated media. Participants shared examples of fabricated videos impersonating journalists and public figures, illustrating how AI technologies can be used to spread false narratives and damage reputations. Because such content frequently uses the likeness of well-known personalities, it can easily mislead audiences and erode public trust in legitimate information sources. At the same time, the session recognized that AI can also contribute to addressing misinformation. Emerging solutions such as AI watermarking, automated detection systems, and fact-checking chatbots are being developed to help identify manipulated content and support verification efforts. However, participants emphasized that these technologies are still evolving and require further development and integration with human-led verification processes.

From a governance perspective, participants underscored the important role of governments in addressing the harmful use of AI technologies, particularly in regulating deepfakes and coordinated misinformation campaigns. However, enforcement measures alone were considered insufficient. Effective responses require collaboration among governments, technology companies, civil society organizations, and the media to promote responsible AI development and strengthen information integrity. Journalists were also identified as critical actors in countering misinformation. Their role includes verifying digital content before publication, educating audiences about misinformation tactics, and using digital verification tools to identify manipulated media. Strengthening public media literacy was highlighted as another key strategy for building societal resilience against AI-driven misinformation.

Key Takeaways

- AI tools can support information verification but require human oversight to ensure accuracy, contextual understanding, and bias detection.
- Deepfakes and AI-generated misinformation pose growing risks to public trust, particularly during elections and crises.
- AI-based solutions such as watermarking, detection tools, and fact-checking systems are promising but still evolving and require further refinement.
- Journalists play a critical role in verifying information, countering misinformation, and educating the public.
- Strengthening media literacy and public awareness is essential to help citizens critically assess digital information.
- Addressing AI-driven misinformation requires multi-stakeholder collaboration across governments, media, civil society, and technology companies.

Recommendations

- Institutionalize human-in-the-loop verification systems in newsrooms, election monitoring bodies, and digital platforms to ensure AI-generated content is reviewed before dissemination.
- Invest in capacity building for journalists and fact-checkers on digital verification tools and AI detection technologies.
- Strengthen regulatory frameworks to address harmful uses of AI such as deepfakes while safeguarding freedom of expression.
- Promote responsible AI development standards, including transparency and accountability mechanisms for AI-generated content.
- Expand media and digital literacy initiatives to equip the public with skills to identify misinformation and manipulated media.
- Encourage collaboration between governments, civil society, and technology companies to develop coordinated responses to AI-driven misinformation.



The discussion also highlighted the growing threat of AI-generated misinformation, including deepfakes and manipulated media. Participants shared examples of fabricated videos impersonating journalists and public figures, illustrating how AI technologies can be used to spread false narratives and damage reputations. Because such content frequently uses the likeness of well-known personalities, it can easily mislead audiences and erode public trust in legitimate information sources. At the same time, the session recognized that AI can also contribute to addressing misinformation. Emerging solutions such as AI watermarking, automated detection systems, and fact-checking chatbots are being developed to help identify manipulated content and support verification efforts. However, participants emphasized that these technologies are still evolving and require further development and integration with human-led verification processes.

From a governance perspective, participants underscored the important role of governments in addressing the harmful use of AI technologies, particularly in regulating deepfakes and coordinated misinformation campaigns. However, enforcement measures alone were considered insufficient. Effective responses require collaboration among governments, technology companies, civil society organizations, and the media to promote responsible AI development and strengthen information integrity. Journalists were also identified as critical actors in countering misinformation. Their role includes verifying digital content before publication, educating audiences about misinformation tactics, and using digital verification tools to identify manipulated media. Strengthening public media literacy was highlighted as another key strategy for building societal resilience against AI-driven misinformation.

Key Takeaways

- AI tools can support information verification but require human oversight to ensure accuracy, contextual understanding, and bias detection.
- Deepfakes and AI-generated misinformation pose growing risks to public trust, particularly during elections and crises.
- AI-based solutions such as watermarking, detection tools, and fact-checking systems are promising but still evolving and require further refinement.
- Journalists play a critical role in verifying information, countering misinformation, and educating the public.
- Strengthening media literacy and public awareness is essential to help citizens critically assess digital information.
- Addressing AI-driven misinformation requires multi-stakeholder collaboration across governments, media, civil society, and technology companies.

Recommendations

- Institutionalize human-in-the-loop verification systems in newsrooms, election monitoring bodies, and digital platforms to ensure AI-generated content is reviewed before dissemination.
- Invest in capacity building for journalists and fact-checkers on digital verification tools and AI detection technologies.
- Strengthen regulatory frameworks to address harmful uses of AI such as deepfakes while safeguarding freedom of expression.
- Promote responsible AI development standards, including transparency and accountability mechanisms for AI-generated content.
- Expand media and digital literacy initiatives to equip the public with skills to identify misinformation and manipulated media.
- Encourage collaboration between governments, civil society, and technology companies to develop coordinated responses to AI-driven misinformation.

Conference way forward

Title: Regional action plan for responsible data governance in East Africa

Panelists from left

- Mercy Kimalat – CEO, Association of Startup and SMEs Enablers of Kenya (ASSEK)
- Linet Kwamboka – Institute for Development Data
- Dr. Emmanuel Mkilia – Director General, Personal Data Protection Authority, Tanzania
- Jedidah Wakonyo – Director and Chief Executive, Kenya Witness Protection Agency (KWPA)



The panel session focused on the future of data governance in East Africa, examining how regional actors can move from policy dialogue to practical implementation. Moderated by Al Kags, Founder and Executive Director, Open Institute, the session explored the challenges of harmonizing regulatory frameworks, strengthening digital sovereignty, protecting sensitive data, and enabling responsible innovation within the region's growing digital economy. The panel brought together perspectives from government regulators, civil society, the startup ecosystem, and justice institutions, highlighting the diverse interests involved in shaping a responsible and inclusive data governance ecosystem. Central to the discussion was the recognition that while East African countries had developed numerous policies, laws, and strategies, the critical challenge lay in operationalizing these frameworks and translating them into effective systems and infrastructure. The discussion examined the intersection between data protection, economic development, technological innovation, and human rights, while emphasizing the need for regional cooperation and practical mechanisms for cross-border data governance.

Key discussion themes

Regional Harmonization of Data Governance Frameworks

The discussion opened with a question directed to Dr. Mkalia, focusing on the fragmented nature of data protection regimes across East Africa and what the first practical steps toward harmonization should be. Dr. Mkalia emphasized that technological connectivity across the region was already achievable, noting that the infrastructure required to connect East African countries through fiber networks and digital systems largely existed. However, the primary challenge lay in regulatory alignment, particularly regarding cross-border data flows. He explained that harmonization should begin with the development of regional mechanisms governing cross-border data transfer, which would establish:

- Common safeguards for data transfers
- Mutual recognition of regulatory standards
- Clear responsibilities for organizations handling data across jurisdictions

Dr. Mkalia further highlighted ongoing efforts by data protection authorities in East Africa to strengthen cooperation, noting that regulators from several countries had begun meeting regularly to discuss shared challenges and develop coordinated regulatory approaches. He stressed that regional collaboration among data protection authorities was essential to ensure consistency in enforcement and to build trust among citizens and investors participating in the digital economy.



In addition, he noted that effective regional data governance could significantly reduce infrastructure costs, arguing that harmonized standards could allow countries to share resources such as data centers rather than duplicating investments in every jurisdiction.

Data Governance and Justice Systems: Protecting Sensitive Information

The moderator then invited Jedidah from the Kenya Witness Protection Agency to discuss the implications of data governance for institutions responsible for protecting witnesses in criminal justice processes. Jedidah emphasized that data security was central to the integrity of witness protection systems, noting that the exposure of sensitive information could compromise investigations, endanger individuals, and undermine the justice process. She introduced the concept of “data justice”, arguing that discussions about data governance must go beyond compliance and consider how data systems actively protect vulnerable individuals. One of the critical challenges she highlighted was the need to ensure the “right to be forgotten”, particularly for protected witnesses whose identities must be concealed permanently or temporarily for safety reasons. This often involved the identity modification data obfuscation, secure data management systems, and controlled access to sensitive records.

Jedidah explained that witness protection programs operate in highly sensitive environments where digital exposure can create significant risks, which is why many systems still rely on manual or non-digital processes. However, she acknowledged that as the world increasingly shifts toward digital systems, witness protection agencies must also adapt, requiring new technological solutions designed specifically to support confidential operations. She called for greater collaboration between technology developers and justice institutions, urging innovators to design digital tools that incorporate witness protection safeguards from the outset.

Ethical Data Use and the Startup Ecosystem

The discussion then shifted to the role of technology startups and the broader innovation ecosystem, with Mercy Kimath providing insights from the perspective of entrepreneurs and technology enablers. Mercy explained that Kenya’s startup ecosystem has grown rapidly over the past decade, particularly following the development of early innovation hubs and digital infrastructure that supported entrepreneurship. She noted that startups across East Africa are now operating in sectors including:

- Agriculture technology
- Health technology
- Green technology
- Circular economy innovations
- Digital financial services

However, she pointed out that access to research data remained one of the biggest barriers to innovation, with many entrepreneurs struggling to obtain reliable datasets needed to develop new products and services. Another major concern she raised was data security, particularly for startups developing intellectual property based on proprietary datasets. Many companies currently relied on international cloud platforms to store sensitive data, which raised concerns about data sovereignty and national oversight.

Mercy emphasized that governments must work collaboratively with the innovation ecosystem to develop data governance frameworks that support innovation while protecting citizens’ rights. She argued that responsible data governance should include:

1. Transparent data-sharing standards
2. Enforcement mechanisms for misuse of data
3. Public–private collaboration in designing data systems
4. Investment in national digital infrastructure

She also highlighted the importance of regional collaboration, noting that Kenya's role as a digital hub could help drive best practices across East Africa if governance frameworks were properly aligned.

Digital Sovereignty and Infrastructure Investments

Another major theme of the panel centered on digital sovereignty and infrastructure development, with Linet Kwamboka reflecting on the broader structural challenges facing African digital ecosystems. She emphasized that discussions about sovereignty must be grounded in realistic assessments of national capacity, including infrastructure, technical expertise, and investment. Kwamboka noted that although many countries emphasized the importance of data sovereignty, the region still relied heavily on foreign digital infrastructure, including cloud platforms and data storage services. She also highlighted the need for strategic investments in education, research institutions, and technological development, arguing that African countries must build the capacity required to develop and manage their own digital systems. Also she expressed concern that many governments continued to prioritize policy development over practical implementation, noting that numerous frameworks and strategies already existed but often failed to translate into real technological advancements. She called for a shift toward investment in innovation ecosystems, including support for entrepreneurs, universities, and research institutions capable of developing locally relevant technologies.

Key Takeaways from the Panel

The panel concluded with several key insights regarding the future of data governance in East Africa:

1. Regional cooperation is essential for managing cross-border data flows and building a trusted digital economy.
2. Data governance frameworks must prioritize citizen protection, ethical data use, and accountability.
3. Governments must move beyond policy development toward investment in digital infrastructure and innovation ecosystems.
4. Sensitive sectors such as justice systems require specialized data governance mechanisms that prioritize security and confidentiality.
5. Collaboration between governments, innovators, civil society, and regulators is necessary to build inclusive and sustainable digital systems.

The session ultimately emphasized that responsible data governance in East Africa will depend not only on regulatory frameworks but also on practical investments in infrastructure, skills, and regional collaboration mechanisms.





PRESENTATION OF CONFERENCE OUTCOMES

Closing Session and Key Reflections

The conference concluded with a reflective closing session that brought together the key themes, lessons, and forward-looking reflections emerging from the two-day discussions.

- Speakers underscored the importance of strengthening data governance, trust, innovation, and regional collaboration, while emphasizing that the next phase for the region must move beyond dialogue toward practical implementation and coordinated action.
- A central message from the closing remarks was that East Africa has made significant progress in developing legal frameworks, policy architectures, and regulatory structures for data protection and digital governance. However, speakers emphasized that the real challenge now lies in operationalizing these frameworks and ensuring that policies translate into real systems, institutions, and practices that benefit communities.
- Participants reflected on the increasing number of data protection policies across the region and questioned whether the existing policy architecture adequately addresses the evolving needs of societies and digital economies. While progress has been made, there is a growing recognition that implementation gaps remain a major obstacle to effective data governance.
- Speakers also discussed the growing number of reported data breaches and privacy concerns across the region. While this trend may signal increased awareness and improved reporting mechanisms, it also highlights the need to strengthen compliance systems, enforcement capacity, and institutional accountability.
- Another important point raised during the closing session was the role of Data Protection Impact Assessments (DPIAs). Participants questioned whether conducting DPIAs alone is sufficient, or whether in some cases they risk becoming procedural compliance exercises rather than meaningful safeguards for protecting individuals' privacy. The speakers therefore encouraged institutions to adopt privacy-by-design approaches, ensuring that privacy considerations are integrated into the design and architecture of digital systems from the outset. Trust emerged as one of the most significant themes throughout the conference.
- Speakers noted that mistrust among governments, civil society organizations, technology actors, and communities can undermine collaboration and slow progress in digital governance. Strengthening trust through transparency, accountability, and open dialogue was therefore emphasized as essential for effective regional cooperation.
- Participants were also reminded that data governance must ultimately be understood as a human-centered issue. Behind every dataset are real individuals and communities whose rights, dignity, and safety must be protected. As such, data governance frameworks must prioritize human rights, ethical standards, and community engagement.
- The closing remarks further emphasized the importance of ensuring that vulnerable and marginalized communities are included in digital governance discussions. Issues such as technology-facilitated gender-based violence, digital exclusion, and unequal access to digital infrastructure were highlighted as areas that require sustained attention and policy action.



As the East Africa Data Governance Conference 2026 came to a close, participants reaffirmed the importance of the forum as a critical platform for advancing regional dialogue, collaboration, and knowledge exchange on data governance across East Africa. There was strong consensus that the conference should continue to evolve as a sustained and action-oriented regional platform, bringing together diverse stakeholders to shape inclusive and accountable digital futures. Participants expressed broad support for maintaining the conference as a rotational regional convening, with different East African countries hosting future editions. This approach was recognized as essential for deepening regional ownership, strengthening cross-country learning, and ensuring that data governance conversations reflect the diverse contexts within the region.

In line with this commitment, plans were announced to convene the next edition of the conference in late February or early March, with proposed host locations including Dodoma and Entebbe, as part of ongoing efforts to broaden participation and regional representation. The closing session also provided an opportunity to express appreciation to all those who contributed to the success of the conference. Participants acknowledged the efforts of the organizers, service providers, moderators, speakers, and partners whose dedication and coordination ensured a well-executed and impactful convening. Special recognition was given to the moderators and speakers for facilitating rich, insightful, and forward-looking discussions that shaped the outcomes of the two-day event.

Key Concepts and Reflections

1. **Policy Architecture**

- East African countries have developed multiple policies and strategies on data governance.
- However, questions remain about whether these frameworks fully address the needs of communities and digital economies.

2. **Data Protection and Governance**

- Increased reporting of data breaches may indicate stronger awareness and monitoring.
- At the same time, it highlights the need for deeper institutional capacity and enforcement mechanisms.

3. **Data Protection Impact Assessments (DPIAs)**

- Participants questioned whether DPIAs are always implemented meaningfully.
- There is a need to ensure they function as real safeguards rather than procedural checkboxes.

4. **Trust and Transparency**

- Trust among stakeholders is fundamental for effective data governance.
- Transparent processes and open dialogue are necessary to strengthen collaboration.

5. **Privacy by Design**

- Privacy considerations must be integrated during the design stage of digital systems.
- Systems should not attempt to retrofit privacy protections after deployment.

6. **Data as a Human Story**

- Every data point represents real people and communities.
- Governance frameworks must therefore prioritize human rights and dignity.

7. **Innovation and Rights**

- Digital innovation must be balanced with accountability and protection of rights.
- Ethical technology development remains a core principle.

8. **Inclusion**

- Vulnerable and marginalized communities must be meaningfully involved in data governance processes.
- Digital transformation should not deepen existing inequalities.

9. Collaboration and Breaking Silos

- Governments, civil society, academia, and the private sector must work together.
- Cross-sector collaboration is essential for building resilient governance systems.

Important Examples and Emerging Issues

1. Technology-Facilitated Gender-Based Violence
2. Digital platforms and applications should be designed to detect and prevent technology-enabled abuse from the outset.
3. Regional Data Governance Policies
4. East Africa has strong policy foundations, but challenges remain in harmonizing frameworks and ensuring consistent implementation.

Key Questions Raised During the Conference

- Are existing policies sufficient to govern the rapidly evolving digital environment?(Focus on policy effectiveness and adaptability.)
- Does increased reporting of data breaches indicate stronger awareness or rising vulnerabilities?(Focus on monitoring systems and institutional capacity.)
- Are Data Protection Impact Assessments meaningful safeguards or compliance exercises?(Focus on the depth of implementation.)
- How can trust be strengthened among governments, civil society, and technology actors?
- (Focus on stakeholder collaboration.)
- Does data protection enable innovation or restrict it?(Focus on balancing policy and innovation.)
- How can marginalized communities be included in digital governance processes?(Focus on equity and inclusion.)

Core Principles and Key Takeaways

- Implementation Must Follow Policy: Effective data governance requires moving beyond policy development to practical implementation.
- Trust Is Fundamental :Strong relationships between institutions and communities are essential for sustainable governance.
- Human-Centered Governance: Data governance must protect the rights and dignity of individuals and communities.
- Continuous Engagement:Dialogue among stakeholders must continue beyond the conference.
- Regional Cooperation: Harmonized approaches across East Africa will strengthen the region's digital economy.



Group photo: conference organizers

Photo Highlights-Day 2



Breakout sessions



Participants networking



Appreciation moment to the Mater of Ceremony and service providers for successful execution and support for the conference



Group photo: conference participants

Notable Quotes

Technology has two dimensions: the drive for innovation and digital advancement, and the human beings at the center of it. While technology continues to evolve rapidly, people—with their dignity, rights, emotions, and experiences—must never be treated as mere products within the digital ecosystem.

Dr. Emmanuel Mkilia, Personal Data Protection Commission, Tanzania

The best approach to balancing innovation and accountability in data governance is a multistakeholder approach. To broaden the regional dialogue beyond data protection to issues of ownership, sovereignty, ethics, interoperability, and the economics of data, all actors must be involved.

Immaculate Kassait, Data Commissioner, Office of the Data Protection Commissioner, Kenya

Data governance cannot be done in silos. It requires collaboration between regulators, practitioners, technologists, academics, and citizens. Only through working together can we create systems that are both innovative and accountable

Dr. Mugambi Laibuta, Data Privacy and Governance Society of Kenya

Data is the currency of the future, but if that currency is not distributed equally, many people will be left behind. Women and girls must be part of the data economy—not as subjects of data, but as creators and leaders within it.

Lady Marième Jamme, Founder, IamtheCODE

Innovation grows where trust is built. Data protection is not a barrier to innovation, it is the foundation that allows people and institutions to trust digital systems.

Immaculate Kassait, Office of the Data Protection Commissioner, Kenya



Notable Quotes

No country can effectively govern data in isolation. Data flows across borders, and so must our cooperation if we are to build resilient and trusted digital ecosystems

Edna Kasozi, Personal Data Protection Office, Uganda

We are collecting enormous amounts of personal data, yet many people still do not understand how that data is used or how it should be handled. Awareness remains one of the biggest gaps in responsible data governance. Across East Africa we have laws, policies, and frameworks for data governance. The real challenge now is implementation, turning these frameworks into everyday practice.

Al Kags, Executive Director, Open Institute

Regulators and practitioners must learn to speak with each other, not at each other. Dialogue between those building systems and those regulating them is essential if we are to achieve balance

Dr. Mugambi Laibuta, Data Privacy and Governance Society of Kenya

Digital identity is no longer just a passport or a national ID. It is also the trail of data we generate every day online—data that increasingly influences decisions about our lives

Panel Discussion Reflection

Skills equal freedom. If people know how to collect data, analyze it, visualize it, and share it responsibly, they gain the power to shape their own future in the digital world.

Lady Marième Jamme, Founder, IamtheCODE



Contact Details:

Phone: [+254 707 673 664](tel:+254707673664)

Email: hello@openinstitute.africa

Address: [9 Riverside, Nairobi Kenya](#)

Website: www.openinstitute.africa