DATA PROTECTION AFRICA SUMMIT 2023

REPORT

Building Bridges for Oversight and Accountability

dataprotectionafrica.org

The Data Protection Africa Summit 2023

Contents

The Data Protection Africa Summit 2023

The 2023 Data Protection Africa Summit (DPAS) is the 6th Summit to be organised by the African Digital Rights Hub (ADRH). The very first DPAS was organised in the year 2018. This year's DPAS took place in Accra, Ghana. The event took place in the last month of 2023, from 12th – 15th December at Labadi Beach Hotel. The theme of the event was "Building Bridges for Oversight and Accountability".

The initial plan was to hold the 2023 DPAS in Morocco, as was revealed at the end of 2022 DPAS in Johannesburg, South Africa. However, due to unavoidable reasons, we were unable to have it in Morrocco. However, to ensure that the Summit would still take place, and that stakeholders, once again, would convene to discuss pertinent issues touching data protection and governance in Africa, the ADRH worked extra hard to find an alternative venue. It was not an easy task, but because the ADRH vowed to provide this platform every year, we worked extra hard to ensure that the DPAS would happen. Indeed, we were able to consolidate our efforts and organise a successful event in Accra, Ghana.

We thank the hardworking ADRH team that worked day and night to make the 2023 DPAS possible. In a very special way, we thank all panellists and keynote speakers who accepted our invitation and showed up – physically in Accra, Ghana or virtually. Your intellectual contribution to the DPAS is highly valued. We would also like to extend our appreciation to Chief Justice of the Republic of Ghana, Her Ladyship Justice Gertrude Torkonoo for accepting to officiate the event and for preparing an opening speech which was read by Justice Jennifer Abena Dadzie on her behalf. Justice Jennifer Abena Dadzie, we thank you for delivering Her Ladyship Justice Gertrude Torkonoo's speech. Your commitment and support in advancing digital rights in Africa is evidenced by your readiness to show up at very short notice and speak at the 2023 DPAS.

Last but not least, we thank our sponsoring partners, the William and Flora Hewlett Foundation, Meta, Google, Margins ID Group, Africa Digital Rights Hub, Nsiah Akuetteh & CO, AB & David, ISACA Accra Chapter and our audience, whether they attended physically or virtually. We say, you are the heart that pumps the life into the Data Protection Africa Summit.

Day One

Part One: Opening Ceremony

The event began with the Master of Ceremony Mr. Nhyira Addo welcoming participants and invited guests. As usual, this was followed by a special performance – a traditional dance and a national anthem. Ms. Teki Akuetteh – the Executive Director of the Africa Digital Rights Hub (ADRH), who are the organisers of the Data Protection Africa Summit (DPAS), gave an opening remark and handed it over to H.E. Thomas Kwesi Quartey for a welcoming address. The welcoming address was followed by a keynote address by Her Ladyship Hon. Justice Jennifer Abena Dadzie who represented the Chief Justice of the Republic of Ghana, Her Ladyship Justice Gertrude Torkonoo. Hon. Justice Jennifer Abena Dadzie's address concluded the welcoming remarks, which was marked by a photo opp and tea break.

Welcome Address by H.E. Thomas Kwesi Quartey

The 2023 Data Protection Africa Summit kicked off with a welcoming address by H.E. Thomas Kwesi Quartey, representing the Executive Council of the Africa Digital Rights Hub.

In his opening remarks, H.E. Quartey emphasised the paramount importance of privacy and data protection in today's digital landscape. He shed light on the potential risks associated with unauthorised access and misuse of personal data, emphasising the all-important need for robust measures to uphold fundamental rights and freedoms.

H.E. Quartey outlined the summit's agenda, which included tackling pressing issues such as cross border data transfers across Africa, implementation of personal identification systems and the vital role of data protection in digital trade. He encouraged the audience to actively participate in the discussions and have a dialogue that can result in improving and advancing data and digital rights in Africa. He also urged everyone to use this opportunity to create networking opportunities, insisting on the summit's role as a platform for sharing insights and fostering collaboration. He concluded his short but very impactful remarks by extending a warm welcome to all attendees to the Summit.

Keynote Address by Hon. Justice Jennifer Abena Dadzie

The keynote address in the opening speech of the 2023 DPAS was delivered by Hon. Justice Jennifer Abena Dadzie. Hon. Justice Dadzie delivered the address on behalf of the Chief Justice of the Republic of Ghana, Her Ladyship Justice Gertrude Torkonoo. Ladyship Justice Gertrude Torkonoo's keynote speech highlighted the multifaceted challenges that most African countries face in safeguarding the privacy and security of citizens' data, and why these unique challenges must be addressed head-on. Some of the challenges, include limited resources, inadequate legislation and a lack of awareness. She further emphasised that the latter poses huge obstacles to effective oversight mechanisms.

In support of the 2023 DPAS theme, "Building bridges for oversight and accountability" Hon. Justice Dadzie called for various stakeholders to recognise the urgency of these issues and the need for collaborative efforts to overcome them. In addition, she intimated that collaborative effort by all stakeholders goes a long way in the creation of a comprehensive framework that would uphold data protection principles and ensure accountability from all stakeholders.

Hon. Justice Dadzie noted that building a bridge for oversight and accountability is a complex process. A process that entails the need to think outside the traditional notion of regulatory enforcement and compliance. She narrated one of the complexities to be the ever blurring of boundaries and transcending nature of personal data. An aspect that would require the recognition of various stakeholders and the roles they play to guarantee the fundamental rights to privacy of citizens. As such contribution and inclusion of all stakeholders is necessary. This includes citizens and individuals whose understanding of the law and vigilance will prompt entities (such as regulators), CSOs and the Judiciary to action.

In another breath, she posed a question to stakeholders on how citizens' data would be protected beyond our boundaries, keeping in mind the current digital technologies, global communication networks and international business practices. In this, case, she insisted that this would also require oversight and accountability beyond borders and local jurisdictions. In this endeavour, she emphasised collaboration at the regional, continental and international levels. She insisted that the safety and free movement of data beyond our boundaries will ensure sustainable socio-economic development.

Flipping the coin, Hon. Justice Dadzie acknowledged and praised the progress that African countries have made in data protection oversight and accountability on the continent. She referred to Ghana’s strides in this score, identifying the enactment of comprehensive legislation on personal data protection, establishment of an independent data protection authority and a fostered culture of transparency and accountability. However, she, once again, insisted on collaboration saying that effective data protection oversight and accountability cannot be taken in isolation, and that for that reason, African countries must come together, transcend borders and share best practices.

In conclusion, she called on all the stakeholders present at the Summit to seize the opportunity to build bridges for oversight and accountability in data protection, and harness the power of collaboration, innovation and cooperation to create a future where the privacy and security of personal data are protected. Finally, she commended Ms. Teki Akuetteh, the Executive Director of the ADRH, and the convenors of the Summit for coordinating an extraordinary Summit and declared the Summit open.

Part Two: Keynote Speech Session

Keynote Speech One: Generative AI & Data Protection in Africa

by Steve Woods,
Director & Founder at PrivacyX Consulting

Mr. Steve Woods who delivered his keynote speech virtually from London highlighted the intersection between Generative Artificial Intelligence (GenAI) and data protection, particularly within the African context. His speech commenced with a reflection on the exponential growth of GenAI globally, and its myriad applications across various sectors. He acknowledged the dual nature of GenAI, and its potential to revolutionise societies while also posing inherent risks.

The discussion then pivoted to the vital role of data protection in promoting AI safety. Woods underscored the importance of upholding data protection principles, such as fairness and data minimisation, within the framework of AI governance. He emphasised the need for a nuanced approach to navigate the complexities of GenAI by balancing the wonder and panic that it brings.

The speech delineated the multifaceted landscape of data flows within GenAI ecosystems. It outlined responsibilities of various actors, including data providers, developers and deployers. On the one hand, it highlighted the significance of transparency, fairness, security, accountability and user rights in mitigating associated risks, and on the other hand, it emphasised on the need to address ethical, legal and societal implications in the deployment of GenAI.

In the African context, Woods spoke of the importance of context in conducting GenAI risk assessments, in developing GenAI governance frameworks, as well as in capacity-building initiatives. He also stressed on the importance of community engagement and indigenous perspectives in shaping responsible AI ecosystems on the continent.

Woods reiterated three things:

- The need for proactive measures to mitigate data protection risks and promote responsible AI adoption in Africa.
- Collaboration among regulators, businesses and civil societies in developing tailored governance frameworks and in addressing capacity gaps effectively.
- Prioritising research agenda that integrates local perspectives, leverages and existing initiatives to inform about AI development and regulation in Africa.
- The urgency in empowering stakeholders with resources and expertise needed to navigate the evolving AI landscape responsibly.

This keynote speech provided valuable insights into the relationship between GenAI deployment and usage, and the role of data protection in fostering safety, ethical and inclusive AI ecosystems in Africa. His comprehensive analysis on related risks and pragmatic recommendations underscored the imperative of collective action to harness the transformative potential of AI while safeguarding individual rights and societal well-being.

Panel Discussion on Generative AI and Data Protection in Africa

The keynote address on *Generative AI and Data Protection in Africa* was followed by a panel discussion. The panel was moderated by Mr. Serge Ntamack and with him as panellists were Mrs. Drudeisha Madhub - Data Protection Commission for Mauritius (who joined online); Mr. Darlington Akogo - founder and Chief Executive Officer of minoHealth AI Labs (also joined online); Dr. Ololade Shyllon - head of privacy policy for Africa Middle East and Turkey at Meta; Mr. Matthew Martin - founder of Two Candlesticks and a cyber security and strategic advisor; and Ms. Jenna Franklin - a lawyer, senior corporate data protection and privacy specialist, and partner at Stephenson Howard LLP.

AI fever and AI Regulation in Africa

Mr. Ntamack initiated the discussion with a narrative 'story' about 'AI fever' happening across the globe. Given the specialized jargons on the theme, he insisted on the use of simple and plain language in clarifying what AI was and its potential impact, risks and challenges for the audience. He initiated the discussion on the fact that regardless of the fear of AI spreading, there are regulatory efforts to ensure that AI deployment and use brings more benefit than harm to human beings. Data protection laws provide a set of principles to ensure that before personal

data is used, there is fairness, transparency in the use, consent, lawfulness of the use of data and accuracy of data to avoid misrepresentation.

After the laying of foundational bricks to the discussion, the panel discussion began. The discussion began by answering the question on whether Africa is well equipped to address AI challenges.

In response, the panel highlighted the fact that AI challenges are not just prominent in Africa but are being faced across the world. This is in line with the fact that AI has brought legal and ethical compliance challenges, controversies with other regulatory fields such as intellectual property rights and impacts so many other legal aspects that the world was not prepared for. However, the discussion emphasized on the fact that most African countries have data protection laws that have core principles which are relevant and applicable to AI regulation. In addition, the African Union (AU) has put together a framework to address the numerous data protection concerns on the continent. One of these initiatives being the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The panel pointed out that the Malabo Convention is not a binding law to AU member states, nevertheless, it provides a blueprint for a regulatory framework in the protection of personal data. Malabo Convention, unlike any other, has a very ambitious coverage and a forward-looking way to regulate the protection of personal data in the digital era and it support innovation.

Panellists acknowledged the fact that potential gaps which may have not been anticipated during the law-making process may still exists. And since AI and innovation in general is faster than regulatory actions, specific gaps would need to be addressed as they come and specifically.

Challenges in Regulating AI and Technology in Africa

The panel dug deeper into specific challenges facing Africa in regulating AI. One of them is the weak implementation of the data protection laws. The panel also offered some recommendations to remedy this. It called for cooperation between political powers of Africa and the AU in finding ways to overcome this challenge. Another suggested approach to regulate AI is for the creation of a clearance framework that will have the mandate to assess and clear the deployment of AI technology in Africa, in the context of Africa's unique settings and cultural contexts. The clearance aspect could lay guidelines, check and licence AI deployment to prevent deployment of potential harmful AI or making Africa a dumping ground for harmful AI technologies.

The discussion rounded back to the idea that technological development is faster than regulatory action. In this, the panel noted that the biggest problem with generative AI is that nobody knows how to use it, and because nobody knows how to use it, frameworks and regulations are layered over these technologies, which limits what the technologies. The same thing is happening in Europe. The panel stressed on the need for key players to come up with frameworks and policies that will guide the conversation rather than enacting laws that will become obsolete in a few years. The panel also saw the need to understand AI and its usage instead of focusing too much on regulating AI itself. This understanding is based on the logic that it makes more sense to regulate the things we create using AI rather than regulating AI itself. But, if we choose to regulate it, then such regulation should not be too detailed. The regulation should take a principle-based approach to allow its application to a wide range of generative AI and related technology.

AI Regulation: A Comparative and Innovative Narrative

In comparing AI regulatory approaches in Africa with other regions the panel used the European Union (EU) approach as an example. In this case, the binary approach to AI regulation taken by the EU in the EU AI Act was brought in. An approach very much in favour of regulating technologies such as AI systems that focuses on strict enforcement, just like the EU General Data Protection Regulation (GDPR). This stringent approach to AI regulation under the EU AI Act is different from other frameworks with more flexible principles such as those adopted by countries like the US, UK and the G7. These softer principles aim to regulate AI by focusing on risk mitigation, identifying appropriate safety measures and addressing vulnerabilities.

The panel also discussed other frameworks such as the Hiroshima AI Principles and the OECD AI Principles. The Hiroshima AI Principles framework is structured around addressing three key areas of vulnerability in the deployment and use of AI technology: the climate crisis, global education and health. In the end, the panel was of the view that Africa could consider a range of principles and frameworks to adapt and come up with its model. In any case, the panel insisted on the need for such regulatory framework to foster innovation, enhance people's lives and protect their rights. In this regard, one of the panellists gave an example of the Mauritius' Data Protection Law which is technology neutral and capable of regulating new technologies. The law has a provision that prohibits subjecting a person to automated decision-making. This provision upholds an important right that every person should have, especially in making decisions. The right not to let the machine make decisions that affects persons. In addition, it was noted that the office of the data protection in Mauritius undertakes compliance audits for some AI developers who are developing AI to assess their compliance with the Data Protection Act. The country has also vamped up tech regulation by adopting specific regulations for FinTech and the Virtual Assets Initial Tokens Act which regulates the licencing of AI technologies. To support these efforts, the country has established an AI Ethics Committee and Emerging Technologies Council at the national level. One of the tasks that the former committee does is to develop guidelines for AI and the latter spearheads research on AI and develop appropriate AI training.

At this point, it was necessary for the panel to give an illustration on how the data protection principles could be applied to AI industry. To elaborate this, a panellist used Meta Platforms to illustrate the matter. Meta Platforms has come up with five (5) responsible AI pillars. These pillars are privacy and security, fairness and inclusion, robustness and safety, transparency and control, and accountability and governance. The five principles are implemented across all AI-related technologies at Meta.

To support in applying such an approach, some advice to use sandboxes was given. This is one effective way to protect privacy without hindering innovation. Sandboxing enables the testing of AI in a controlled environment, allowing the identification of potential gaps and issues, which provide designers with the opportunity to make necessary improvements. An important aspect is the necessity to understand AI, its uses and the outcome we desire. In this case, we should ask ourselves, "for what purpose is the AI going to be used?" The answer to this question will enable the deployment of AI in a way that its decisions are explainable and auditable.

The discussions came to an end at this point to enable the audience to interact with the panellists.

Interactive Session on Generative AI & Data Protection in Africa

The panel discussion was followed with an interactive session where the audience contributed to the keynote speech presented and ideas that stemmed out of it.

> **Question 1:** The audience wanted to know how generative AI can be adopted into education, teaching, learning and research.

The answer used an innovative tool called LLAMA (Large Language Model Meta AI) Impact to elaborate, The LLAMA Impact was developed by Meta to address challenges in education, public services, healthcare and safety. It is an AI tool like ChatGPT, a foundational model that people can build on. In terms of improving education delivery, the tool can be used to increase access to quality education and enhance the teaching experience. This can include AI-powered tutoring, personalised learning platforms and intelligent teacher tools.

LLAMA Impact was launched as an innovative award offering financial support to organisations that can use it to innovate solutions in three main categories and these categories are education, environment and innovation. The education aspect, supports innovative ideas to support students and teachers.

On general terms, generative AI has been used to access the overtime score of students, helping them to understand issues and explain things to them when they are trying to figure out a particular topic. It supports both students and teachers in aspects like assessments and preparing for academics.

Question 2: The participant from the audience asked whether a pre-given consent from a data subject can be leveraged further to process that subject's personal data within the scope of generative AI models.

One of the panellists narrated how difficult it is to satisfy the criteria for consent for processing personal data. An example of a case that took place in Italy was given in this regard. In this case, the Data Protection Authority in Italy stopped ChatGPT from using consent as the basis for its processing of personal data. The authority stopped the processing of personal data for Chat GPT purposes because those processing such information could not satisfy the consent requirements as per existing law. Realistically, the use of personal data for generative AI is mostly recommended to be done based on 'legitimate interest' rather than on 'consent'. However, even under legitimate interest, one must satisfy the legitimate interest assessment. This means that the processing of personal data in this context does not outweigh the interests of the data subject.

Question 3: Another participant wanted to know if the Malabo Convention provides sufficient frameworks to regulate generative AI.

The response from the panel noted that the Malabo Convention does not address many AI concerns, issues and safeguards. An upgrade is needed on this. However, it was the AU has developed the AU Data Policy Framework. The framework complements the Malabo Convention framework by including recommendations on regulating data processing in the digital services and context, including AI. However, the panel insisted on the need to streamline legislation across Africa to support harmonisation in data protection and AI regulation. In this case, the regulators have a very big role to play by providing support to the African Union in legislative harmonisation.

Question 4: Once again, a question on the use of AI in education settings came up. This time, the participant wanted to know whether there are measures put in place to regulate the use of generative AI in education. In clarifying the question, this participant said she asked the question because she is a teacher whose students use generative AI to generate answers to questions asked in school.

In response, the panel insisted on the need everyone to take initiative to reduce harm that might be a result of AI use, in this case teachers must adapt to these new ways of doing things, including the use of technologies such as AI. Furthermore, there is a need for schools/teachers to come up with guidelines/guiding principles on what students can and cannot do with AI. In reality, students are going to look up and research on their assignments, whether its via Google, encyclopaedia or even ChatGPT. So, teachers should adjust to these new technologies and think about functional ways to assess knowledge that yields similar or intended goals.

From a legal point of view, the panel reminded the audience that the school is basically a data controller, and it is important for schools to ascertain the accuracy and authenticity of the information that is being provided by a student. There should be ways to see if students have relied on ChatGPT during an exam.

Question 5: A question that followed was on data monopoly and data protection by big tech companies. The audience wanted to know how big tech companies such as Microsoft, Google and Meta ensure the balance between data protection and their business or commercial interest in the use of generative AI since these big tech companies have access to and process huge amounts of data in this regard.

Given the nature of technology, the discussion from the panel insisted the need for not just the companies that created the (AI) tool are responsible but also that every single person using that tool should be required to do so responsibly. So, by focusing just on big tech companies and those providing innovative tools, such as AI, we might be probably missing the point.

Question 6: The last question for this session centred on the fear of continued advancement in AI technologies. The participant wanted to know if humans will be replaced when AI becomes a separate legal entity and if so, are these systems going to acquire rights.

The response insisted on the need to prevent AI from becoming a separate/ independent legal entity because that will mean extending human structures to AI systems – including the rights and duties structures.

At this, the moderator called for a midday break to allow presenters and participants to re-compose themselves, have lunch and network before the event resumed for the next session.

Keynote Speech Two: Building a Trust Framework for Data Transfer Across Africa

by Mrs. Drudeisha Madhub,
Data Protection Commissioner, Republic of Mauritius

Mrs. Drudeisha Madhub, the Data Protection Commissioner of the Republic of Mauritius, delivered a keynote address for the second session of the first day. The focus of her keynote speech was on the significance of the African Continental Free Trade Agreement (AfCFTA) and the African Union (AU) data policy framework in shaping a trust framework for data transfer across Africa. She started by highlighting key articles within the AfCFTA that facilitate cross-border data flows in Africa, emphasising on specific aspects such as harmonisation, equivalence, cooperation, protection and confidentiality.

In addition to the AfCFTA as a framework promoting trust for cross-border data flows, she emphasised the importance of implementing the African Union Data Policy Framework (DPF) towards harmonised policies framework across African countries and facilitate trade on equal terms. Beyond Africa, Mrs. Madhub briefly touched upon international documents such as the European Union General Data Protection Regulation (GDPR) and the Convention 108+, on their impact in safeguarding cross-border data transfer laws. In this light, she stressed the significance of aligning African policies with global standards while strengthening regional collaboration to ensure data protection and security on the continent.

Mrs. Madhub concluded her keynote speech with six strong recommendations towards building a safe and secure framework for cross-border data flow for Africa:

- Harmonisation of Policies: Implement the DPF to harmonise policies across African countries and facilitate trade on equal terms.
- Cooperation and Interoperability: Foster cooperation among public, private and civil society entities to promote exchange, interoperability and coherence in data systems across Africa.
- Data Protection Impact Assessments: Require data protection impact assessments before deploying new technologies to mitigate the risks and harm associated with processing data.
- Promotion of Sector-Specific Needs: Promulgate codes of conduct to address sector-specific needs and ensure best practices in mitigating risks associated with processing data.
- Incorporating Local Perspectives: Prioritise a research agenda that integrates local perspectives and leverages existing initiatives to inform about AI development and regulation in Africa.

- Bilateral and multilateral trade agreements: Given the lack of harmonisation in data protection laws in Africa, cross-border trade agreements should include data protection clauses ensuring fair and equal participation in cross-border data flows on the continent.

Panel Discussion on Building a Trust Framework for Data Transfer Across Africa

Following the keynote speech, five experts joined Mrs. Madhub on a panel discussion to debunk points she advanced in her keynote speech. The panel discussion was moderated by Mr. Samuel Bartels. Mr. Bartels introduced the panellists (alongside Mrs. Madhub) to include Dr. Patricia Boshe, Mr. Baker Birikujja, Mr. Serge Ntamack and Ms. Jenna Franklin.

The moderator started the session by asking why the conversation on ***Building a Trust Framework for Data Transfer Across Africa*** is crucial. Before he allowed the panellists to respond, he gave a provocative response to the question by saying the conversation is crucial given the fact that data access, sharing and use is becoming a key economic driver, and that with it comes the amplification of the various concerns and risks relating to the transfer of data back and forth across the globe. As a result, the issue of trust must be discussed because it's at the core.

Creating Trust in Cross-Border Data Flow

The panel began the discussion on the theme 'trust between African countries and the big tech organisations.' To clarify this, the panel first elaborated that trust is a shared responsibility. In this case, a responsibility between countries and big tech.

In as long as technology-oriented-machinery promote access to information collection, it must ensure that trust framework is embedded in the process. Unfortunately, this is not the case in majority of cases. As a result, creating trust is big challenge. Lack of trust deepens where there is

no transparency from data processors and controllers with their consumers. In the end, customer's trust is neglected for commercial profits. So, basically, trust issues mainly emanate not from the government nor consumer, but the controllers and processors of data, and that for that reason there is a need for regulation of corporate activities and advocate for corporate responsibility towards data protection.

On the current 'state of trust' the panel used the ever-emerging data localisation policies on the continent as an indication of the idea that trust levels are lowers. Countries are attempting to recover lack of trust by implementing data localisation policies to protect personal data of their citizens. Unfortunately, these policies are the biggest hurdle to digital economy. Data localisation policies are, in essence, saying 'I do not trust you with my data, and therefore, I would retain my data within my local boundaries.' The challenge of this approach is that it limits or restricts cross-border data flows. If one country does not trust the other to allow free flow of data (by imposing data localisation rules), how can the other country have trust in its counterpart to let its data flow freely to that country?

If data localisation laws are too stringent, they affect companies and decrease their productivity. Data localisation deepens the mistrust among industry players and countries. In as much as the companies have a role in nurturing trust, governments need re-think and develop related policies carefully not to impede on data flows or data sharing, but at the same time, ensure data protection to foster trust among and between countries.

Navigating Cross-Border Data Flows: Africa and Beyond

After this, the moderator asked about barriers to moving data across countries in Africa? The main challenge that the panel noted in this regard is the existence of different laws and legal frameworks that data controllers need to comply with. Lack of harmony in policy and legislation brings frustration in cross-border data flows within the continent. To transfer data across different African borders, quite often, start-ups would need to seek a unique framework which they can sign on to deal with the various jurisdictional obstacles.

The panel also noted that lack of harmonisation is not only a challenge in Africa, that similar challenges are faced in other regions such as in the EU and UK. This meant that Africa can also look into and learn how other regions are dealing with the challenge. The panel also opined that there is no perfect solution to ensuring trust in the transfer of data across borders. However, establishing a central body of governments where discussions are held to work through an approach to enhance the free flow of data could be a start towards establishing trust among African countries.

African Union and Cross-Border Data Flow

The moderator re-directed the discussion by asking the panel's opinion on whether they think African countries overlooked economic effects and priorities in the process of implementing [policy] decisions that affect data transfer across the continent?

By using the AU Data Policy Framework, the panel illustrated how AU developed a policy framework that not only prioritize policy alignment on the continent but very much takes cognizance of the different economic levels the member states are in. The AU Data Policy Framework seeks to ensure free flow of data across the continent without leaving one behind, and leave behind economic protectionism, data colonisation, etcetera.

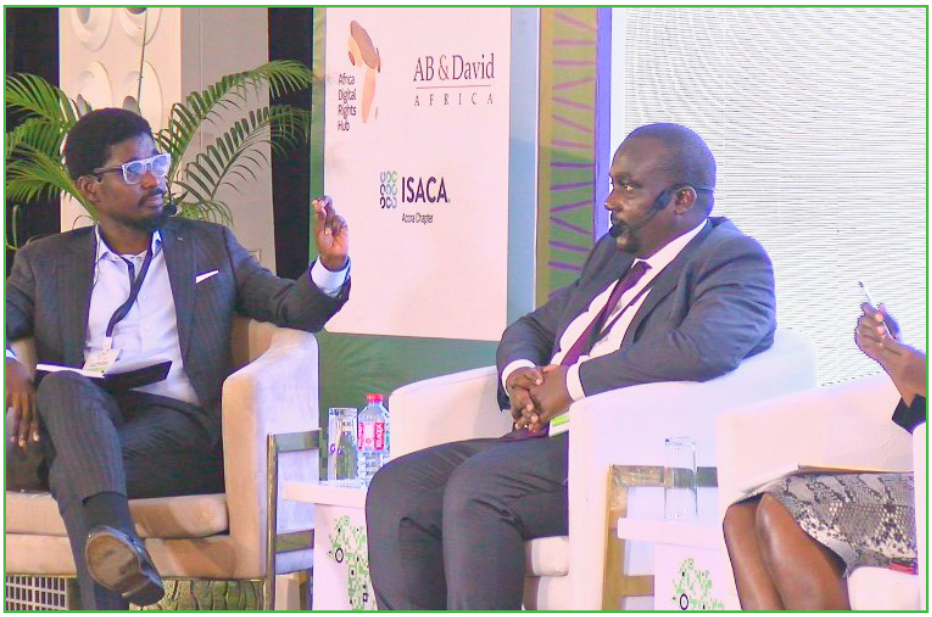
Cross-Border Data Flow in Africa: The Way Forward

The panel continued the discussion by exploring means and approaches to support trusted cross-border data flows. One of the panellists used an example of Uganda to initiate the discussion. In Uganda, cross-border data flow framework is a 'conditional one' in that data controllers and processors who wish to transfer data outside Uganda must make an assessment to ensure the recipient country or organisation provides an adequate level of protection similar to the one provided by Ugandan Data Protection Act. In addition, data controllers and processors are required to register with the regulator and make an oath before a commissioner of oaths declaring that they will not transfer personal data to a country that does not have similar laws or protection, as accorded in Uganda.

The panel discussion narrated the need for the AU, as the regional organisation, to bring African countries together and be able to come up with a mechanism of transferring personal data across borders – at least on the continent. The discussion emphasized on the fact that such a mechanism should have at least three things: It must create a ***transparent framework, be predictable*** and impose some amount of ***accountability*** on actors. In addition to the three, there is a need for a centralised approach and cooperation between governments to ensure that both public and private organisations across the continent are held accountable for their activities.

Regardless of challenges facing the continent the panel showed optimism about Africa's journey towards a trusted framework for a cross-border data flow. This is based on the fact that more than have of the countries with data protection laws have established data protection commissioners who play a primary role in ensuring trust. If these authorities could come together and decide on a certain framework that can support cross-border data flow, that will be an effort worth pursuing. However, to have a workable framework on a continent with diverse legal approaches, there is a need to agree on flexible rules that take cues of different judicial cultures and backgrounds rather than adopting a rigid one-size-fits-all framework.

In addition, the panel insisted of the need of governments' involvement and support to data protection authorities' endeavours to protect personal data beyond borders. Noting that, government support is inevitable as implementing data protection laws has a political undertone to them.



Interactive Session on Building a Trust Framework for Data Transfer across Africa

The panel discussion was followed with an interactive session where audience members were given a chance to contribute to the dialogue.

> **Question 1:** How do we get more countries involved to help build trusted frameworks for data protection on the continent?

In responding to this question, the panel highlighted the importance of cooperation between enforcement authorities which they considered to be a step towards building trusted frameworks. Question 2: The audience wanted to know whether data protection regulators in countries across Africa can be trusted to enforce data protection laws.

In answering this question, the panel noted that enforcement has been one of the major challenges for data protection authorities on the continent. The regulators not only enforce the law but are expected to play multi-functional roles in regulating the industry. Regardless of these challenges, the regulators are doing their best to enforce these laws. The evidence is the many enforcement activities taking place on the continent. In addition, to dialogue between regulators, processors and controllers and capacity building and education initiatives taken by the regulators to educate all stakeholders on the data protection ecosystem before sanctions are imposed.

To narrate this, an example of Uganda and Mauritius was given. In Uganda violations of the data protection law is a crime which attracts punitive sanctions and is prosecuted by a prosecutor. This feature of the law builds trust amongst states. Also, the Personal Data Protection Office in Uganda has a special Court assigned by the Chief Justice to deal with privacy offences. This shows how serious enforcement of data protection law is taken.

In Mauritius, in 2018, the regulator introduced mediation as one way to resolve data protection disputes amicably. This approach was introduced because of the realisation that case prosecutions take a lot of time, energy and resources, and they involve a lot of intricacies associated with judicial rules and procedures. This approach proved to be very promising and is working very well.

> **Question 3:** The third question was a re-enforcement of the second question where the audience wanted to get a comparative perspective: How the European Union has been able to enforce its laws and what can Africa learn from them.

The panel started by cautioning against comparing Africa with Europe in terms of data protection enforcement. This is because the two continents are not on the same level on the matter. Europe has had its first comprehensive data protection law in force since the late 1970's. Europe has a long-standing experience, and they have learned through time. However, on the African continent, the first comprehensive data protection law came about in 2001. So, Africa still has time to learn to see how our context is affected and how to better incorporate it into the laws.

In addition, the two continents have different strengths of power and ability in terms of enforcement. The European Commissioners have the power to enforce, for example, their directives on countries and sanctions them in case a country fails to enforce those laws, but the African Union does not have that power. In effect, the African Union depends on the political will of countries to enforce the laws out of goodwill.

Question 4: A follow-up question from the audience. A participant wanted to know, 'At what point will the African Union be able to sanction countries that break the [data protection] laws since Africa is lagging because there is no central authority to enforce the laws?'

To answer this question, the panel elaborated that the powers AU have are statutory [law-based]. The instrument that created the AU needs to give AU such powers and this will need a consensus from member states. This means, for AU to have such powers would require instrumental changes before institutional change. We will require to go back to the instrument that established the African Union, amend or re-draft it to give the African Union such powers.

In addition, the African Court being has limited enforcement powers over African countries. For the Court to hear a case against a certain country, that country must have signed the Court instrument to give the Court power to adjudicate upon it. Again, to change this, we must go back to the documents that created the Court.

Question 5: Lastly, the panel were asked to share their experiences in terms of incentivising African governments to take a step towards not just ratification, but also enforcement.

One of the points of view given was that the biggest incentive is when a country sees interest, either from a security or economic perspective. For example, the reason why many countries are ratifying the AfCFTA is because they have seen economic interest which is tangible. The problem countries have with data protection is that they cannot really conceptualise it as it is very technical. So, for many countries, data protection does not really translate into immediate monetary incentive. It may not necessarily be economic incentive, and there is no definite answer to 'incentive' but that it is a combination of various interests that can incentivise governments to enforce data protection laws.

Another point raised is the support from the government and peer pressure. In the latter, governments may be encouraged to adopt and adhere to a protocol or law when most countries have adopted it. This marked the conclusion of the discussion and the first day which was followed by a networking session over soft drinks and snacks.

Day Two

Part One: Keynote Speech Session

Day two of the event started right away with keynote speeches. The day consisted of two keynote speeches and a closing ceremony which entailed a special performance, acknowledgements and appreciations, closing remarks and the unveiling of the Venue for the next Data Protection Africa Summit.

Keynote Speech One: Data Protection Implementation in the Delivery of ID Systems in Africa

by Teki Akuetteh,
Founder and Executive Director – Africa Digital Rights Hub

Ms. Teki Akuetteh presented a keynote address for the first session of the second day of the summit. In her address, she spoke on Ghana's ID ecosystem, the inclusiveness and exclusiveness of national ID frameworks in other West African countries, the Data Protection Code of Practice for digital ID schemes, and how these laws must be simplified to ensure that people understand their implication.

In this light, she spoke about privacy rights and about why data protection is important to the ID ecosystem. She also explained the potential dangers in the deployment of digital ID systems such as infringement of personal privacy and misuse of personal data, exclusion from accessing basic needs or exercising civic rights and identifying theft and identity-based discrimination. On the other side, she illustrated the importance of data protection laws in overcoming most of these concerns. She noted that when data protection laws are properly implemented, they could promote personal privacy, safety and security of personal data during the deployment and usage of National IDs in Africa. She said that the implementation of data protection laws means taking advantage of the great benefits IDs could offer whilst minimising the potential abuse and risks to individuals and their personal data.

Data protection plays a pivotal role in the whole process of collecting information for the National IDs system, she noted. To illustrate this point, she referenced the Supreme Court of India case ***Justice K.S. Puttaswamy v Union of India*** where the court insisted that through the implementation and use of the Aadhaar scheme (India ID system), the government must recognise the privacy rights of individuals and ensure their protection.

Ms. Akuetteh underscored the importance of openness and transparency when rolling out ID systems. These afford the citizenry with the nature of the data processing activiting involving their personal data. In fact, openness and transparency are among the mandatory principles under data protection laws, she said. Beyond openness and transparency, there is a need for an accountability framework. In this case, she noted the importance of organisational accountability in achieving inclusiveness.

To further clarify her point above, Ms. Akuetteh narrated the three different phases in the deployment of an ID scheme. These are the enrolment phase, issuance phase and the life cycle management phase. She insisted that in each of the three stages, there is a data protection element to be enforced to prevent breaches. Openness, transparency and accountability are a step towards ensuring data protection in the three different phases of the deployment of ID systems.

Ms. Akuetteh then brought in Ghanaian context. She identified the key principles that ID systems must comply with to ensure the individual data protection is safe. They include accountability, openness, authorisation or consent, collection of good quality and updated information, collecting as minimal data as necessary for the purpose, and providing access to data subject to correct information. These are principles found in the Data Protection Act of Ghana. Consequently, she, once again, emphasised on the importance of data protection when deploying ID systems, and as one of the critical tools needed to create the right balance between the issuing of IDs and the development, deployment and safety of the individuals whose IDs are being issued.

Ms. Akuetteh's keynote speech provided valuable insight into the ID ecosystem in Ghana (specifically) and Africa (in general). The keynote speech also offered insights into ensuring safety and inclusiveness in the ID ecosystem in Africa.

Panel Discussion on Data Protection Implementation in the Delivery of ID Systems in Africa

The panel discussion was moderated by Dr. Sena Afua Dei-Tutu and featured insights from key experts including Dr. Patricia Boshe, Theresa Eson-Benjamin and Kholofelo Kugler. The discussion revolved around the complexities and challenges of implementing data protection measures in the African context, particularly with national identification systems and the influence of international regulations.

Experiences with National Identity Systems in Africa: Kenya and Ghana Under Review

The moderator started the discussion by asking the panellist o their experience with digital IDs in Africa. An experience from Kenya with the ***'Huduma Namba'*** and ***'Maisha Namba'*** ID systems stood out. The Kenya ***Huduma Namba*** and ***Maisha Namba*** initiatives as digital ID systems were met with significant public outcry due to concerns about data privacy and the potential for misuse of personal information. The rollout of ***Huduma Namba***, which was intended to streamline government services by assigning a unique identification number to every citizen, was contentious.

One of the major issues raised by citizens was the lack of clarity and transparency regarding how their data would be used and protected. Despite assurances from the government, many Kenyans feared that the centralised collection of personal data, including biometrics, could lead to surveillance or unauthorised access. This fear was not unfounded as there had been previous instances of data breaches and misuse in other government projects.

The situation escalated to the point where civil society organisations and human rights groups took legal action against the government, challenging the constitutionality of the ***Huduma Namba*** system. They argued that the system was introduced without sufficient safeguards to protect citizens' privacy and violated fundamental rights enshrined in the Kenyan Constitution. The court responded by temporarily halting the implementation of the system until proper data protection measures were put in place.

In response to these concerns, Kenya enacted the Data Protection Act in 2019 to address the gaps in privacy and security. However, the public's scepticism persisted. Many citizens remained wary of the government's ability to protect their data, given the lack of prior trust and the rapid implementation of the ID systems without comprehensive public consultation. At this point, the panel insisted the fact that a mere existence of data protection laws is not enough to alleviate public fears; the governments need to actively demonstrate its commitment to protecting privacy through transparent practices and consistent enforcement of the law.

During the discussion, the panel also highlighted the broader implications of the Kenyan experience for other African nations considering similar national ID initiatives. It was clear that while digital identification systems have the potential to improve service delivery and governance, they must be implemented with a strong foundation of trust. This trust can only be built through meaningful engagement with the public, clear communication about the purpose and use of data, and robust legal and technical frameworks that ensure data security and privacy.

Additional insights from the National Identification Authority (NIA) of Ghana were shared. The discussion dwelled into how Ghana navigated similar concerns as in Kenya. Like Kenya, in Ghana, the Data Protection Act of 2012 serves as the primary legal safeguard for personal data in country. The law outlines principles and govern the collection, storage and use of personal data. Accordingly,

NIA's operations have been guided by this law, ensuring that the personal information of millions of Ghanaians is handled with care and in compliance with international standards.

Beyond alignment with the data protection law, NIA ensures that individuals are fully informed about how their data will be used and has implemented strict access controls and data management protocols to prevent unauthorised access or misuse of personal information. NIA also implements other technical measures safeguard personal data such as the use of encryption technologies, secure data centres and regular security audits. In addition, data systems are designed to be resilient against cyber threats, with multi-layered security protocols that protect the integrity and confidentiality of the data collected.

It was also noted that, NIA adheres to data minimisation, collecting only the data necessary for identification and service delivery. This approach not only reduces the risk of data breaches but also aligns with the principle of privacy by design, ensuring that data protection is considered at every stage of the ID system's development.

In addition, in acknowledging the role of social policy in fostering public trust NIA engages the public through awareness campaigns, ensuring that citizens understand their rights under the Data Protection Act and the measures in place to protect their data. These public engagements have been crucial in addressing concerns and building confidence in the system. This underscores that idea that that trust is not just built through laws and technology, but also through continuous dialogue with the people who are affected by these systems.

At this point, the panel circled back to that fact that laws and practices on the continent lack uniformity. This, as argued by the panel, creates challenges for cross-border cooperation and the harmonisation of data protection standards, especially as more African countries move towards digital identification systems. The panel also noted that the rapid pace of technological advancement means that data protection strategies must be constantly reviewed and updated to address new risks.

The conversation highlighted that while Ghana's experience provides valuable lessons, there is no one-size-fits-all solution. Each country must tailor its approach to its unique context, balancing the need for effective identification systems with the imperative to protect citizens' privacy rights.

Regional and Continental Data Protection Frameworks Maze

The panel discussion moved into the broader context of regional and continental frameworks for data protection in Africa, with a focus on how these frameworks can be leveraged to address the challenges posed by the continent's diverse and fragmented legal landscape.

Africa is a continent of diversity with 55 countries, each with their own legal and regulatory systems; this makes the task of harmonising data protection laws across the continent incredibly complex. This diversity contrasts sharply with regions like the European Union where a more uniform approach to data protection has been achieved through the General Data Protection Regulation (GDPR). In addition, and in contrast to Europe, Africa has several Regional Economic Communities (RECs). Some of the RECs with their own data protection frameworks. This means beyond the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention), we have the East African Community's (EAC) cyber laws framework, ECOWAS Act, and SADC Model Law. Navigating this patchwork of different regulations is a challenge.

Additionally, the Malabo Convention, which was adopted in 2014, its impact has been limited by the slow pace of ratification among African Union member states. The fact that diminishes the Convention's potential to create a unified approach to data protection in Africa.

The discussion then turned to the African Continental Free Trade Area (AfCFTA) protocol on digital trade, which the panel believe could serve as a platform to address these gaps and support alignment in regional data protection efforts. The AfCFTA, aims to create a single market for goods and services across Africa, and includes provisions for digital trade that could be expanded to cover data protection. By incorporating strong data protection measures into the AfCFTA, African countries could create a more cohesive and integrated approach to data protection that aligns with global standards, while also addressing the unique needs of the continent.

One of the key points raised during this part of the discussion was the importance of building on existing frameworks rather than starting from scratch. Panellists agreed that Africa's diversity should be seen as a strength rather than a weakness. By leveraging the experience and expertise of countries that have made significant progress in data protection, such as Ghana and Kenya, a more tailored and effective continental strategy could be developed.

The need for capacity building and knowledge sharing among African countries was also emphasized. Many nations, particularly smaller or less developed ones, lack the technical expertise and resources to implement and enforce robust data protection laws. Regional and continental organisations, such as the African Union, could play a crucial role in providing support and training to these countries, helping to bridge the gap between different levels of development across the continent.

Another aspect the discussion focused on was the role of international cooperation and the influence of global data protection standards. The GDPR was frequently cited as a model, not just because of its comprehensive approach to data protection, but also because of its extraterritorial reach, which continue to compel companies and countries outside the EU to comply with its standards. Panellists discussed whether Africa could develop a similar approach that would allow it to exert influence on a global scale, particularly in negotiations with international technology companies and other stakeholders.

During this discussion, the panel recognised the challenges of implementing such a framework. The question of sovereignty loomed large as many African countries are hesitant to cede control over their data protection laws to a supranational entity. This reluctance is compounded by historical factors, including the legacy of colonialism, which has left many African nations wary of external control. Regardless, the panel saw the need for a greater cooperation and harmonisation as a strategy that can ultimately lead to stronger protections for African citizens and more competitive economies.

The discussion on regional and continental data protection frameworks underscored the need for a balanced approach that respects national sovereignty while promoting regional cooperation. By building on existing frameworks and fostering greater collaboration, Africa can develop a data protection strategy that meets the needs of its diverse populations and aligns with global best practices.

The Potential for a Supranational Data Protection Framework

The panel discussion then delved into the complex and potentially transformative idea of establishing a supranational data protection framework for Africa, akin to the European Union's General Data Protection Regulation (GDPR). This topic sparked a lively debate among the panellists and attendees, who weighed the pros and cons of such a framework and its feasibility in the African context.

To lay the foundation of the discussion, the concept of a supranational framework was clarified. This is when a central authority would oversee and enforce data protection regulations across multiple nations. The idea that many believed would represent a significant shift from the current situation, where individual African countries have their own data protection laws—if they have any at all. A supranational framework could help harmonise these laws and ensuring a consistent standard of data protection across the continent.

The discussion highlighted one of the primary advantages of such a framework to be the creation of a unified digital market in Africa, where businesses could operate across borders without the complexities of navigating different national regulations. This could spur economic growth, attract foreign investment and boost innovation by providing a clear and predictable legal environment for digital businesses. Moreover, a supranational framework could strengthen Africa's bargaining power on the global stage, allowing it to negotiate better terms with international technology companies and ensure that the data of African citizens is protected in alignment with global standards.

However, the discussion quickly turned to the challenges of implementing such a framework. The panellists acknowledged that Africa's political and legal diversity makes it difficult to establish a central authority that could effectively enforce data protection laws across the continent. This is compounded by the fact that many African countries are wary of ceding sovereignty to a supranational entity, particularly given the continent's history with colonialism and external control.

To add context to the idea, the panel brought in a comparative discussion using the European Union as an example. It was noted that, although the European Union, has a long history of political and economic integration, the GDPR faced significant challenges in its implementation. So, it should not be a surprise for Africa with far less experience with such integration, not to willing or able to adopt a such an approach. In terms of data protection enforcement, in the EU, the GDPR is enforced by national data protection authorities, but these entities are supported by a strong legal and institutional framework at the EU level. In Africa, where many countries lack the necessary infrastructure and expertise, enforcement would be a major hurdle. Without effective enforcement mechanisms, a supranational framework could end up being more of a symbolic gesture than a practical solution.

The conversation then touched on the potential for regional blocs within Africa, such as the East African Community (EAC) or the Economic Community of West African States (ECOWAS), to take the lead in developing and enforcing data protection standards. This regional approach could serve as a stepping stone towards a more comprehensive continental framework. By starting with smaller and more cohesive groups of countries, Africa could build the necessary legal and institutional capacity before scaling up to a continent-wide framework.

However, the panel cautioned that any move towards a supranational framework would require extensive consultation and buy-ins from all stakeholders, including governments, businesses and civil society. The process must be inclusive and transparent to ensure that the framework reflects

the needs and concerns of African citizens. This would also help to build trust in the system, which is essential for its success.

In the end, the panel agreed that while a supranational data protection framework for Africa holds significant potential, it also faces substantial challenges. The idea is ambitious and would require careful planning, strong political will and extensive cooperation among African nations. The panel emphasised that any move towards such a framework must be driven by African needs and values, rather than simply replicating models from other parts of the world. They also called for further research and dialogue to explore the feasibility of this approach and to develop strategies for overcoming the challenges identified during the discussion.

The panel discussion underscored the need for stronger and more cohesive frameworks that considers the continent's unique challenges. While national efforts like those in Kenya and Ghana show progress, the discussion highlighted the necessity for regional and continental collaboration to create a more secure and trusted digital environment in Africa.

The panel concluded with a call for further research and dialogue to address the existing gaps and to consider the potential benefits of a supranational approach to data protection in Africa.

Interactive Session on Data Protection Implementation in the Delivery of ID Systems in Africa

After the panel discussions, the moderator welcomed the audience for an interactive session.

Question 1: The session began with a question on the validity of the digital IDs.

A participant from the audience wanted to know whether IDs should last forever without expiring as it is in countries such as South Africa, Botswana and Rwanda. The participant clarified the basis of the question, saying 'stakeholders should consider an ID system which does not expire since the human information remains unchanged, as this will save stakeholders some cost.'

The question was specific to the Ghana ID system and so the answer was as well directed to that specific context. Accordingly, the audience was informed that the Ghana Card is valid for ten (10) years. The ten-year limit is based on the card becoming brittle after this period. Although person's biometric data in the system remains/might remain the same, the card is to be renewed every ten years to capture any change in status of the individual over the years, and the renewal does not require going through the whole process all over again.

Question 2: The second question was on the relationship between the National Identification Authority (NIA) and the Death and Birth Registry (BDR) of Ghana.

This question was also answered in the specific context, i.e. Ghana. It was explained that the BDR is set up to capture all incidence of birth and death in Ghana. To register with the NIA, one must present their original birth certificate or passport. In the absence of these IDs, a relative who has been issued with a Ghana ID must vouch for such person or any two (2) persons in the absence of a relative. For verification purposes, not just anyone can vouch for you. It must be by a person approved by law. [The law lists the persons who are eligible to verify one identity for the purposes of registration by the NIA]. Before an update is made on information contained in the NIA database, the NIA will confirm from the Birth and Death Registry to satisfy itself on the authenticity of the certificate being presented. There are circumstances whereby the Criminal Investigation Department will be asked to conduct such investigations and if it turns out to be authentic, the data will be updated.

The essence of the relationship between the NIA and the BDR is verification. In this case, where people present their birth certificate (even when it looks genuine), the ID is verified by checking with the Death and Birth Registry database to ensure that the document presented is not falsified. This verification process is an ongoing process in post-registration activities to confirm the validity of the details provided. This requirement is also a legal obligation of data controllers. Data controllers are required to make sure that the information they collect is up to date and is relevant to the purposes for which it is being collected. This is not the responsibility of the data user.

Question 3: The third question inquired about the measures which the NIA has put in place to combat vulnerability exposures in its system.

The response from the panel made it clear that no technological system is 100% perfect and that vulnerability will always exist. However, secure the system, best practices must be benchmarked and routine monitoring framework to identify existing and potential system threats must be implemented. Regarding NIAs approach, the system is monitored daily to identify vulnerabilities and is certified to the highest global standards. In addition, NIA is vigilant to monitor it knowing that the system is not 100% perfect.

Question 4: A participant wanted to know where he could find the laws and information about ID users, specifically, the Ghana ID Card.

In this regard, the audience was informed that NIA has summarized relevant laws that individuals need to know about their digital ID cards. Anyone can access and read snippets of these laws on the NIA website.

Question 5: The fifth question in this session was on how to protect an innocent person whose [ID] number has been used to register a SIM card which is being used to commit crimes.

The question reflects a popular misconception and required a clarification on the use of digital ID numbers across ID ecosystem and the role of NIA. In this regard, illustrated to the audience that, SIM registration, including the whole verification process, is not done by the NIA. The NIA is only involved only to verify the existence of the ID PIN [the number] in its database and whether it matches the name assigned to it. But beyond that, the actual verification of where an individual went and when his or her fingerprints were taken and merged to the database, is a technical process not within the ambit of or managed by the NIA but specific vendor, and in case of SIM Card registration, the Telecommunication company.

Question 6: The next question was an inquiry into the applicability of the right to be forgotten in the employment context. A participant posed three questions in this regard.

First, if an ex-employee has the right to demand his or her ex-employer to delete from their database all data relating to him or her.

Second, if an ex-employee must hand over the ID provided by the ex-employer, or if the ex-employee can keep it. And

third, if there is an institution that is ensuring that all institutions are adhering to the data protection laws.

In response, the panel discussion clarified that the institution [ex-employer] is mandated to delete ex-employees' information upon resignation and this right is provided for under the Data Protection Act. In addition, when private institutions are collecting information, especially biometric information of their employees, the institution must inform them of the purpose of collecting such information and how the information is going to be used. An employee has the right to request this data from the institution. Although the practicality and implementation of this right may be a challenge.

This marked the end of the first keynote speech and a break then followed to allow participants and the audience to stretch their feet and grab something to eat and drink, as well as engage in short networking.

Keynote Speech Two: Role of Data Protection in the Implementation of AFCFTA Digital Trade and E-Commerce Protocol

by Teki Akuetteh,
Founder and Executive Director of the Africa Digital Rights Hub

After the break, Ms. Akuetteh gave her second keynote speech addressing the critical role of data protection in the implementation of the Africa Continental Free Trade Agreement (AfCFTA) digital trade and e-commerce protocol. She began by discussing the state of the digital economy in Africa, highlighting the increasing adoption of digital technologies and the emergence of legal and regulatory frameworks to support digital trade.

Ms. Akuetteh identified several challenges hindering the readiness of African countries to fully participate in digital trade under the AfCFTA. Some of the challenges noted include the digital divide, lack of comprehensive policy implementation and ineffective enforcement of data protection laws. She believes addressing these three challenges would improve inclusive participation in digital trade in Africa.

Specific to the AfCFTA and data protection, Ms. Akuetteh identified four key areas that the AfCFTA should address to strengthen data protection and support cross-border data flows and digital trade:

The four areas include:

- The need for harmonisation of data protection laws across African countries to facilitate cross-border data flows.
- The need to establish mechanisms for managing cross-border data flows while ensuring privacy and data protection.
- The need to create trust frameworks and certification systems to build certainty and trust in the data protection ecosystem.
- The need to recognise and address challenges faced by MSMEs in complying with data protection laws. This goes along with the need for tailored support and capacity-building initiatives.

In conclusion, Ms. Akuetteh believes that for the success of the AfCFTA, it is crucial to:

- Simplifying data protection laws,
- Provide clarity on obligations for MSMEs,
- Develop sector-specific guidelines, and
- Create enabling tools to facilitate AfCFTA compliance.

She also suggested the need to incorporate data protection (by default and by design) into innovation industry and start-up activities and exploring the possibility of establishing digital economic free zones based on data protection compliance frameworks within specific countries.

Overall, the keynote speech provided valuable insights into the intersection of data protection and digital trade in Africa, and offered practical recommendations for policymakers, businesses and other stakeholders to address the challenges and opportunities in this area.

Panel Discussion on the Role of Data Protection in the Implementation of the AfCFTA Digital Trade and e-Commerce Protocol

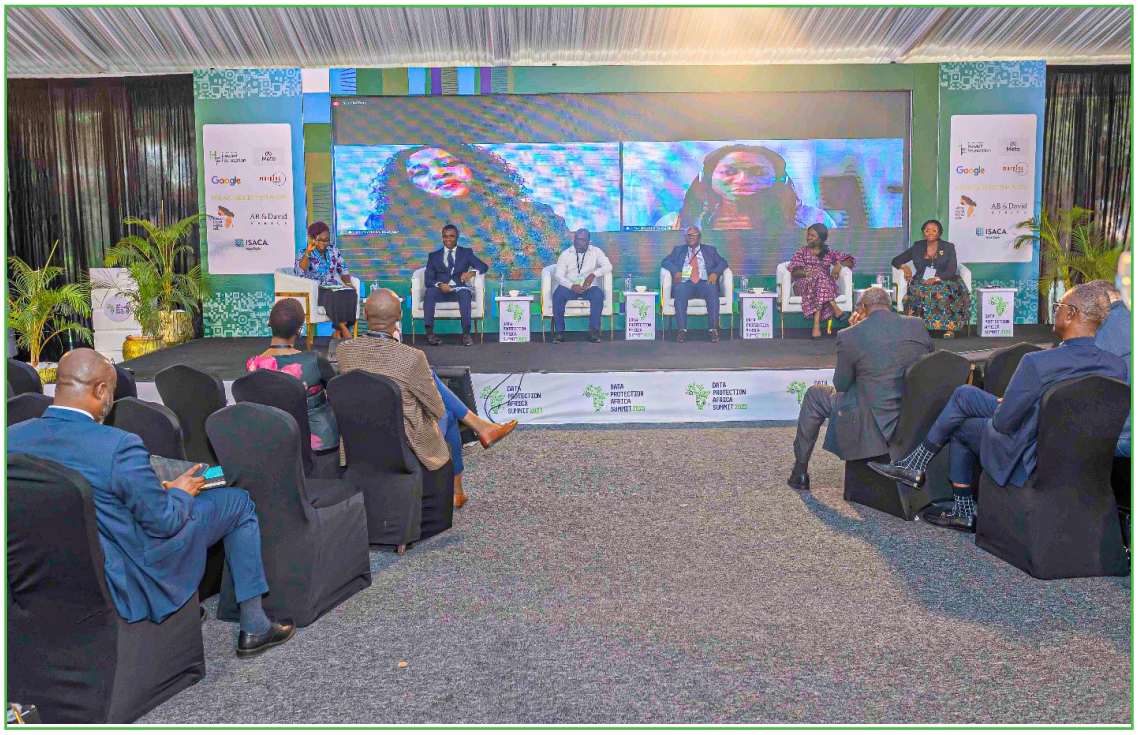
The keynote address was followed by a panel discussion moderated by Dr Sena Dei-Tutu. The panel consisted of Ms. Teki Akuetteh, Mr. Mosalanyane Mosala – the Chief Executive Officer and Information Regulator of the South African Digital Protection Office, Dr Ololade Shyllon - the Head of Privacy Policy of Africa, the Middle East and Turkey of Meta, Stella Nalwoga - International Trade Lawyer focused on digital trade and governance (online), Kholofelo Kugler – International Trade Lawyer and PhD Fellow at the University of Lucerne in Switzerland (online), Mr Francis Kyereh – Cybersecurity Payments and Privacy Consultant, and Mr Silvere Assoua - Head of Compliance and Rights Protection department at the Directorate for Protection of Personal Data (Ivory Coast).

The Role of Data Protection in the Implementation of the African Continental Free Trade Agreement Protocol on e-Commerce and Digital Trade.

The moderator initiated the discussion by introducing the topic to the audience and explaining what data protection is, what the AfCFTA is and what the Digital Trade and e-Commerce Protocol is. She then posed a question to the panel on the role of data protection in the implementation of the African Continental Free Trade Agreement protocol on e-commerce and digital trade.

Before the answer, the panel highlighted the purpose of trade agreements, i.e. to make trade between countries simple. In this case, not only within the physical realm but also within the digital space realm. Data protection play a big role in supporting trade in the digital realm data. Data travel alongside trade. Data protection frameworks set standards on what is needed to enable cross-border data flows to support trade. Data protection is as a safeguard to protect the interests of the consumer and provide businesses legal certainty when they conduct business across borders. Data protection laws provide the minimum standards that are to be expected.

To clarify further the last point, the discussion illustrated how, from a classical trade background, data protection regulations [in Africa] are considered trade barriers. Lack of harmonised regulatory frameworks among countries on the continent is a challenge and raises the cost of compliance. However, we must come to terms with the fact that data protection regulations are required to foster consumer and business trust. Without data protection, trade would be very costly in a longer term.



Lack of Harmonisation in Data Protection Laws as an Impediment to Cross-Border Data Flow and Digital Trade

The moderator brought in a discussion on how lack of legal harmonisation is impeding to the successful implementation of the AfCFTA Protocol. In response, the panel discussion identified one of the fallacies is that technology vendors do not understand the kind of data used in Africa and the regulators are not giving sufficient education to support people in understanding the nature and categories of data used, and what it means under regulatory lenses. Another aspect is the fact that has been repeated during the summit, lack of legal harmonisation. The fact that the continent is populated with conflicting regulations is the number one enemy of the ideas and objectives the AfCFTA is trying to achieve.

Despite the lack of legal harmony, it was noted that, data protection laws in some countries, such as South Africa are geared to support free trade. The preamble of the Protection of Personal Information Act (POPIA) emphasis on enforces this law in a manner that facilitates free trade, innovation and development both in and outside South Africa. However, the panel noted the fact that, some African countries still do not have data protection laws. This is problematic for cross-border data transfer within the continent and a potential impediment to the AfCFTA.

As to the reason why there are still countries with no data protection laws, the panel illuminated that there are many reasons why these countries do not have data protection laws, but that the main reason could be the lack of political will. Solution could involve stakeholders and CSOs pushing for the adoption of data protection laws but that ultimately it is governments that adopt laws. Still, there are some countries that have adopted data protection laws but that they do not implement them due to lack of necessary resources. In addition, there is also the lack of capacity and understanding of the significance of having data protection laws.

The panel insisted that data protection is a necessary aspect in any cross-border trade. Data protection acts as a catalyst for the economy and plays a crucial role in ensuring data security. There is also the need for awareness on data protection and the need to engage the public to ensure such protection.

AfCFTA and MSMEs involvement in Africa

In concluding its discussion, the panel talked about the involvement of MSMEs in the trading process, and how they can benefit from the AfCFTA. The panel recognised the fact that not every business will take advantage of AfCFTA. To support MSMEs taking the advantage of AfCFTA support is necessary, especially to those MSMEs that wants to participate in the cross-border trade. Also, MSMEs, especially those engaged in high-risk sectors should receive data protection education before they are given a licence to operate. The emphasis was on a bottom-up model where regulators consult with big companies on the continent to bring everybody on board. In addition, the panel emphasised on the need to identify challenges faced by MSMEs conducting cross-border trade, especially in the high-risk industries and craft solutions to them. The regulators should engage with personal development agencies to elicit their views and adapt their approach to suit the industries' requirements.

Another recommendation was for data protection regulators to work with other sector-specific regulators to develop a scaled down version of data protection requirements. This is because these sector-specific regulators understand better the businesses within their sector. This collaboration should also feature in educating MSMEs on data protection.

With these recommendations, the moderator welcomed the audience for a more interactive discussion.

Interactive Session on Role of Data Protection in the Implementation of the AfCFTA Digital Trade and e-Commerce Protocol

The moderator initiated the discussion by emphasising on the necessity of regional cooperation to harmonise data protection laws across African nations. She suggested the formation of a supranational entity that could oversee these regulations, like the European Union (EU). The idea revolved around the benefits of ceding a degree of national sovereignty for the greater collective good. The goal is to create a unified framework that ensures data protection while fostering economic growth and technological advancement in the region.

> **Question 1:** The audience wanted to know how we can ensure that this supranational entity respects the diverse cultural and legal landscapes across Africa.

The panel signalled their optimism in the ongoing initiatives like the African Union (AU) Data Policy Framework and the Pan-African Payment and Settlement System (PAPSS). Although political integration might be a gradual process, functional cooperation in areas such as the PAPSS shows immediate promise. These initiatives are steps toward achieving comprehensive data protection and efficient data sharing across borders. They lay the groundwork for a more integrated African digital economy.

Furthermore, the panel noted, despite existing challenges such as enforcing data protection law (especially in the context of cross-border) and the complexities of defining national affiliations under the African Continental Free Trade Area (AfCFTA) having a robust data protection framework that can withstand the pressures of global trade while protecting African interests is necessary.

> **Question 2:** Another participant asked about specific measures that African countries implement to safeguard their data against external economic pressures.

The discussion in answering this question pin-pointed several initiatives by the African Union in addressing various issues, including data protection. The emphasis was on the need for Africa to tailor-made its approaches to reflect Africa's socio-political and economic realities, ensuring that data protection regulations are both effective and culturally relevant. In addition, the panel mentioned some of the initiatives that supports the idea of having tailor-made regulations to African context. It includes the AU Data Policy which aims to harmonise data protection standards across African nations. This policy provides a consistent framework that facilitates cross-border data flows while ensuring data privacy and security. By aligning with international best practices, the AU Data Policy makes it easier for African countries to engage in global digital trade, thereby promoting economic growth and technological innovation.

Question 3: A third question from the audience required specific examples of initiatives towards unifying Africa digital trade.

The response used the example of the Pan-African Payment and Settlement System (PAPSS). The PAPSS is an innovative platform designed to streamline cross-border payments across Africa, reducing the reliance on external financial systems. By providing a unified platform for transactions, the PAPSS promotes economic integration within the continent, enhances financial inclusion and ensures secure, efficient and cost-effective payment processes. This system is particularly beneficial for small and medium-sized enterprises (SMEs) which often face challenges in accessing international financial services.

Another example brought in during the discussion is the Smart Rwanda Master Plan and Kenya's Digital Economy Blueprint which serve as exemplary models for other African nations. These strategies prioritise digital literacy, cybersecurity and the development of a digital infrastructure that supports sustainable economic growth. By focusing on comprehensive digital transformation, Rwanda and Kenya are setting the stage for a more inclusive and secure digital economy.

Question 4: Another participant wanted to know how other African countries can replicate the success stories of Rwanda and Kenya in their digital transformation efforts.

In regards, the role of Regional Economic Communities (RECs) such as the Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS) was highlighted. RECs are crucial in driving regional integration and harmonising data protection laws. RECs facilitate collaboration among member states and help to create a conducive environment for cross-border data flows and digital trade. By working together, these communities can address common challenges and leverage their collective strengths to enhance data protection across the region.

Question 4: Another question was on digital literacy programmes currently in place, and how they support SMEs in Africa in light of digital trade came up.

In this regard, Ghanaian government's Digital Transformation Strategy and Nigeria's Digital Economy Policy and Strategy, were cited. These Strategies focus on enhancing digital skills across various sectors and build a digitally literate society. These strategies provide a bridge to close the digital divide, ensuring that more people can participate in and benefit from the digital economy.

In addition, the panel discussed on the importance of Public-Private Partnerships (PPPs) in promoting digital literacy and supporting SMEs. Companies like Google, Microsoft and Huawei are investing in training programmes and providing resources to help African businesses and individuals develop digital skills. These partnerships are instrumental in fostering an environment of innovation and compliance with data protection standards. In leveraging existing initiatives, promoting digital literacy and supporting SMEs, African nations can create a secure and prosperous digital future. The collective efforts of governments, regional bodies and the private sector are essential in achieving these goals and ensuring that Africa remains competitive in the global digital economy.

Question 5: The audience further brought out a discussion about a malware incident on WhatsApp. In this regard, the audience opined on the need for more robust legal frameworks and international cooperation to tackle cybersecurity threats of similar nature.

The panel agreed on the fact that advancement in technologies come up with new and more complex challenges and that is why we need comprehensive legal frameworks to protect users from cyberattacks and ensuring the integrity of digital systems. Many African countries lack the necessary legal infrastructure to address the complexities of modern cyber threats. Developing and enforcing stringent cybersecurity laws that can effectively respond to these challenges is imperative.

In addition to comprehensive legal frameworks, international cooperation is another vital component that was discussed. Accordingly, the panel noted that, cyber threats do not respect national borders, making it essential for African countries to collaborate with international partners to combat these issues. Organisations such as the African Union (AU) and regional bodies like the East African Community (EAC) and Economic Community of West African States (ECOWAS) play a crucial role in fostering this cooperation. Through joint initiatives, information sharing and coordinated responses, these organisations help strengthen the continent's cybersecurity defences.

Another important aspect discussed in this respect is capacity building in the legal and law enforcement sectors. Many African countries face a shortage of trained professionals who can effectively implement and enforce cybersecurity laws. Initiatives aimed at training judges, lawyers and law enforcement officers in cyber law and data protection are essential. A notable example of such training initiative cited by the panel is the African Centre for Cyber Law and Cybercrime Prevention (ACCP) which provides training programmes and resources to enhance the capacity of legal professionals across the continent.

The public also needs to get awareness and education. The discussion underlined that educating the public about cybersecurity risks and best practices is vital for creating a culture of security. Governments and private sector organisations need to invest in awareness campaigns that inform citizens about how to protect their personal information online. Programmes like Kenya's National Cybersecurity Strategy include public education components designed to increase awareness and promote safe online behaviours was highlighted.

The discussion also addressed the challenge of jurisdiction in cyberspace. Determining which country's laws apply in cases of cross-border cybercrime can be complex. To mitigate this, African countries must harmonise their legal frameworks and develop mutual legal assistance treaties (MLATs) that facilitate cooperation when investigating and prosecuting cybercrimes. In this regard, the Budapest Convention on Cybercrime was cited as a blueprint that could provide a useful outline for such cooperation, offering guidelines for international collaboration when combating cyber threats.

Lack of local infrastructure was also identified as one of the challenges in curbing cybercrimes on the continent. Many African countries rely on foreign technology providers for data storage and processing, raising issues about data sovereignty and the potential for foreign surveillance. The emphasis is to insist on policies that encourage the development of local data centres and technology solutions, reducing dependency on external providers and enhancing control over national data.

Finally, the panel reiterated the role of private sector in bolstering cybersecurity measures. Companies play a vital role in protecting their systems and customer data. Collaboration between the public and private sectors can lead to the development of more robust cybersecurity strategies. Initiatives like public-private partnerships (PPPs) help leverage the expertise and resources of both sectors to enhance overall cybersecurity resilience.

Session Nuggets

- Examples of successful digital literacy programmes include the Ghanaian government's Digital Transformation Strategy, which focuses on enhancing digital skills across various sectors, and Nigeria's Digital Economy Policy and Strategy which aims to build a digitally literate society. These programmes help bridge the digital divide, ensuring that more people can participate in and benefit from the digital economy.

- The importance of public-private partnerships in promoting digital literacy and supporting SMEs cannot be overstated. Companies like Google, Microsoft and Huawei are investing in training programmes and providing resources to help African businesses and individuals develop digital skills. These partnerships are instrumental in fostering an environment of innovation and compliance with data protection standards.

In general, the discussions emphasised the need for greater cooperation and the potential benefits of a unified approach to data protection in Africa. While significant challenges remain, existing initiatives and the collective will of African nations provide a foundation for progress. The discussions highlighted the importance of developing tailored solutions that consider Africa's unique socio-political landscape, rather than attempting to replicate models from other regions entirely. By fostering regional cooperation and creating robust data protection frameworks, Africa can achieve a secure and prosperous digital future.

Closing Ceremony of the 2023 Data Protection Africa Summit

The discussions ended at 5pm GMT. To close the event, Ms. Teki Akuetteh expressed her immense pride in Ghana for hosting the summit and emphasised the importance of the event in advancing data protection and privacy awareness in Africa. She acknowledged the support from key sponsors such as the William and Flora Hewlett Foundation, Meta, Google, Nsiah Akuetteh and Co, AB & David Africa and the ISACA chapter. Ms. Akuetteh highlighted the financial challenges associated with organising such events and thanked the sponsors for their crucial role in making the summit possible.

She also stressed the significance of data protection as more than just a legal requirement but as a cornerstone for Africa's socio-economic development and digital transformation. She underscored the need to ensure inclusivity in the digital space to prevent anyone from being left behind.

She acknowledged the regulators' critical role in guiding data protection efforts and the experts who travelled from various parts of Africa and beyond to share their insights. Her appreciation extended to everyone who took time off their schedules to participate in the summit.

Mr. Nhyira Addo, the Master of Ceremonies for the summit, took over and brought a lively and engaging close to the event. He encouraged attendees to share their experiences from the summit on social media to extend the event's impact and attract more participants in the future. Mr. Addo also shared a personal anecdote about his journey with the Africa Digital Rights Hub, illustrating the evolution of the DPAS and the collaborative spirit that has driven its success. His story highlighted the importance of persistence and vision in realising the goals of data protection and privacy across Africa. He also introduced the team of the Africa Digital Rights Hub and expressed his gratitude for their tireless efforts in making the summit a success.

The closing ceremony concluded with the announcement of the next summit's location. In a moment of anticipation, Mr. Addo revealed that the 2024 Data Protection Africa Summit will be held in Uganda, the Pearl of Africa. This announcement was met with enthusiasm, signalling the continuation of the summit's mission to promote data protection awareness across different African nations.

DATA
PROTECTION
AFRICA
SUMMIT