DATA PROTECTION AFRICA SUMMIT 2024

REPORT

Data Protection Compliance: A Catalyst for Africa's Digital Transformation

dataprotectionafrica.org

Data Protection Africa Summit 2024

Data Protection Compliance: *A Catalyst for Africa's Digital Transformation*

PARTNERS

Personal DATA Protection OFFICE

Meta

WILLIAM + FLORA Hewlett Foundation

Africa Digital Rights Hub

JAMIIFORUMS

NSIAH AKUETTEH & CO

TWO CANDLESTICKS

VinCsys CONSULT

Content

Introduction **6**

Pre-Summit **7**

Early Registration & Master Classes Trainings **8**

DAY ONE 10

DAY ONE: PART TWO 17

DAY ONE: PART THREE 24

DAY TWO: PART ONE 31

DAY TWO: PART TWO 37

CLOSING CEREMONY 41

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY 42

DAY FOUR: HOST COUNTRY TOUR 48

Introduction

The 2024 Data Protection Africa Summit (DPAS) is the seventh edition of this annual event organised by the Africa Digital Rights Hub (ADRH). The 2024 DPAS was organised in collaboration with the Personal Data Protection Office, Uganda. This year's theme was **Data Protection Compliance: A Catalyst for Africa's Digital Transformation.** The ADRH and the Uganda Personal Data Protection Office came up with this specific theme based on the increasing need for and challenges in safeguarding personal data brought by the 4th Industrial Revolution.

The 2024 Summit was a call and a platform for data controllers, users and processors of personal data to discuss pertinent issues and forge solutions towards a more practical and rights-based approach compliance. It was also a reminder to all stakeholders to remain prudent in the management, storage and use of personal data.

As African countries experience the role of data in the 4th Industrial Revolution, with a push to develop strong data protection and data governance frameworks, enforcement authorities are becoming the central piece in ensuring success of the 4th Industrial Revolution, while at the same time, the safety and protection of personal (and non-personal) data is assured. To support this, the 2024 DPAS brought together Data Protection Authorities (DPAs) from several African countries, industry players, practitioners, scholars and other stakeholders in a single platform to identify, discuss and coin solutions that can support innovation, economic growth and data value while placing the rights of data subjects and the need for proper data management in the centre of every data processing activity.

This report is an overview of what happened during the 2024 DPAS, in Kampala, Uganda. The report is produced in an effort to ensure that, even if you missed the event in person, you are able to get a snippet of it, and possibly you are inspired to join us in the future to support and contribute to the development of data governance and the protection of digital rights on the continent.

Pre-Summit

The 2024 Data Protection Africa Summit commenced on 2nd December 2024 with registration and intensive Master Class sessions. Three Master Class sessions were conducted to provide registered participants with training on how to implement some of the data protection and data management requirements of the law in real-life situations. These sessions were not just a warm-up to the actual Summit, but also an important part of capacity building towards data protection, data governance and digital rights implementation.

Early Registration & Master Classes Trainings

The registration with the Summit went parallel with the registration into Master Classes. Participants had options between three Master Classes, namely, Cybersecurity; Data Protection Impact Assessment; and ISO/IEC 27701 Privacy Information Management System. Each Master Class lasted for about four hours and attracted more than 40 participants. At the end of the Master Class, each participant received a decorated certificate of participation. Facilitators and sponsors of the Master Classes are Nsiah Akuetteh & Co., Two Candlesticks and Vincys.

The pre-summit activities provided for logistical preparation and capacity-building opportunities. The day also prepared the grounds for the main Summit days that followed.

We thank the hardworking teams from the ADRH and the Uganda Personal Data Protection Office that worked day and night to make the 2024 DPAS possible. In a very special way, we thank all panellists and keynote speakers who accepted our invitation and showed up – physically in Kampala, Uganda or virtually. Your intellectual and practical contribution to the DPAS is highly valued. We would also like to extend our appreciation to Dr. Amina Zawedde, the Permanent Secretary from the Ministry of ICT & National Guidance, for agreeing to officiate the Summit and for preparing an opening speech delivered by Mr. Kenneth Bergarokayo. Your commitment and support in advancing data governance, protection and digital rights in Africa was seen during the DPAS. To Mr. Bergarokayo, we thank you for your readiness to bless the Summit with your presence and present the opening speech.

This year's Summit was decorated by the presence of the Mayor of Entebbe, Mr. Fabrice Rolinda, who took time out of his busy schedule to welcome participants to the city and the Summit. We are grateful for your support and commitment, not just to the Summit, but also in advocating for data governance and digital rights. In a special way, we thank Mrs. Stella Alibateese, who was the data protection commissioner at the time of the Summit, for working with our team tirelessly and for hosting the Summit. Additionally, we thank you for your welcome speech – all of this illustrates the depth of your commitment to the cause. We would also like to deliver our appreciation to Dr. Philomena Nyarko from Africa Digital Rights Hub for her welcome address, and Mr. Srikanth Mangalam for his keynote address.

Last but not least, we thank our sponsoring partners, including the Personal Data Protection Office of Uganda, the William and Flora Hewlett Foundation, Meta, Africa Digital Rights Hub, Nsiah Akuetteh & Co, the JamiiForums, Internet Society, Two Candlesticks and Vincsys whose support made the event possible. We say, you are the heart that pumps the life into the Data Protection Africa Summit.

On-sight registration for the 2024 DPAS and Master Classes.

DAY ONE

Part One: Opening Ceremony - Opening and Welcome Address

The Summit was commenced by the Master of Ceremony Mr. Kwaku Nhyira-Addo who warmly welcomed participants and guests, and announced the Summit's theme, **"Data Protection Compliance: A Catalyst for Africa's Digital Transformation,"** emphasising the role of data protection in Africa's digital ecosystem. The announcement was followed by the national anthem of Uganda and a prayer, setting a tone of unity and reflection. This was followed by the opening and welcoming speeches from delegated and invited guests of honour.

Welcome Speech

By Mrs. Stella Alibateese – National Director of the Personal Data Protection Office, Uganda

Mrs. Stella Alibateese, the National Director of the Uganda Personal Data Protection Office welcomed participants to the Data Protection Africa Summit 2024. Mrs. Alibateese expressed delight at the diverse gathering of participants, especially from various African Data Protection Authorities. She conveyed the honour of being the host of the 2024 DPAS.

In her speech, Mrs. Alibateese emphasised the importance of data protection compliance in Africa's digital transformation. She noted a continental milestone with more than 50% of Africans with data protection laws. She further insisted on the need to learn from each other, network, and create relationships that can help navigate the digital world and support compliance. She underscored that this Summit is the needed platform to discuss matters related to data protection on the African continent as it brings together a variety of stakeholders from government bodies, regulators, the private sector, civil society, academia, and other organisations to deliberate on those crucial aspects in the data governance ecosystem. She thanked the Minister of ICT & National Guidance, the Africa Digital Rights Hub and its partners for their support in making this event possible in Uganda, and the support of the NITA-U Board and Management for their unwavering support to the Personal Data Protection Office.

Mrs. Alibateese expressed her welcoming remarks by wishing participants fruitful deliberations and encouraging them to enjoy Uganda's best weather, food and vibrant nightlife.

Mrs. Stella Alibateese – National Director of the Uganda Personal Data Protection Office giving the welcoming speech for the 2024 DPAS.

Welcome Address

By Dr. Philomena Nyarko from the African Digital Rights Hub

On behalf of the ADRH, Dr. Philomena Nyarko welcomed attendees to the Summit. Dr. Nyarko gave participants a short introduction to the ADRH's mission, vision and objectives in the data governance and digital rights advocacy across Africa. She highlighted on the fact that the ADRH promotes Afrocentric solutions related to data governance and digital rights on the continent. She mentioned that some of the activities that the ADRH is involved in include advancing and promoting research and advocacy on digital rights across Africa through publications, podcasts and campaigns.

Dr. Nyarko said this Summit is one of the platforms that the ADRH uses to advance its work. Specifically, the Summit aims to explore relevant issues on data protection and privacy in Africa, discuss compliance issues and propose measures or solutions to address those issues and challenges. The Summit does this by bringing together stakeholders to share experiences and proffer solutions. She then encouraged participants to take advantage of the opportunity to learn, share and network with some of the key professionals and practitioners specialising in the field of privacy and data protection, who were present at the event.

Dr. Philomena Nyarko from the African Digital Rights Hub giving her welcoming address at the 2024 DPAS.

Welcome Address

By Permanent Secretary – Ministry for ICT and National Guidance, Uganda

The Permanent Secretary of the Ministry for ICT and National Guidance, Dr. Amina Zawedde, prepared a welcome speech which was delivered by Mr. Kenneth Bergarokayo on her behalf. In the speech, Dr. Zawedde extended her greetings and warm welcome to participants in Uganda.

In her speech, Dr. Zawedde emphasised the importance of data protection, citing this year's theme (Data Protection Compliance, a Catalyst for Africa's Digital Transformation) and noting the vital role data protection compliance plays in unlocking Africa's digital potential and positioning Africa as a leader in the global digital economy.

Mr. Bergarokayo thanked the organisers on behalf of the Permanent Secretary and emphasised Uganda's commitment to data protection through its Data Protection Act and the Personal Data Protection Office. He encouraged collective action, bold thinking, pushing boundaries in data protection and urging stakeholders to work together in making history in data protection compliance.

Keynote Address

By Mr. Srikanth Mangalam - the President of PRISM Institute

Mr. Srikanth Mangalam, the President of PRISM Institute gave a keynote address on the importance of interconnectedness and outcome-based collaboration and trust in achieving better outcomes in data protection compliance.

Mr. Mangalam, who is a globally recognised visionary and expert in risk-informed decision-making, highlighted some key points in data protection enforcement, especially in today's interconnected world.

His address emphasised on the following:

- The Fact That The Use Of Interconnected Systems In The Current Global Economy Results In Interconnected Risks, Means That Collaboration And Trust Among Stakeholders Is Required.
- Regulations Are Essential To Protect Society From Harm And Ensure Public Well-Being. Regulators Must Deliver This Task, Considering The Interconnectedness Of Outcomes And Multiple Regulatory Systems.
- Compliance Is A Means To Achieve Outcomes And Not The Ultimate Outcome. In Interconnected Systems, Compliance Chaos Can Arise Where Compliance Is Made The End Goal. This Stressed The Need For A More Collaborative Approach To Prevent Potential Chaos.
- Trust Is Essential For Collaboration, And Leveraging The Human Ability To Trust Can Lead To Better Outcomes. Conventional Enforcement-Based Approaches Have Limitations, And A More Positive, Trust-Based Approach Is Recommended.
- The Outcome-Based Cooperative Regulation (Obcr) Framework, Developed By Professor Hodges, Which Involves Stakeholders Collaborating Towards Agreed-Upon Outcomes, Co-Developing Codes Of Engagement And Generating Evidence To Demonstrate Trustworthiness, Can Offer A Solution To Compliance Challenges In The World Of Interconnected Systems.
- The Obcr Can Be Applied To Various Sectors, Including Food And Medical Supply Chains, Energy, And The Environment, Which Involve Technology And Digital Aspects Like Ai.
- A Tailored Made-In-Africa Approach To Regulations Is Recommended, Especially In The Digital Space, While Leveraging Universal Concepts Like The Obcr.

He concluded his address by highlighting the importance of shifting from conventional, enforcement-based regulatory approaches to a more collaborative, trust-based approach. He emphasised that by adopting the OBCR, regulators can better address the challenges of interconnected systems, promote public well-being and foster a more positive, collaborative environment.

Data Protection Compliance: A Catalyst for Africa's Digital Transformation
Meta

By Mr. Srikanth Mangalam - the President of PRISM Institute on his keynote address on the importance of interconnectedness and outcome-based collaboration and trust in achieving better outcomes in data protection compliance.

Event Opening Address

By the Mayor of Entebbe

The Mayor of Entebbe, Mr. Fabrice Rolinda, welcomed participants to the summit, acknowledging the importance of protecting personal data. He noted that Africa needs more punitive measures to safeguard data. He also emphasised the need for broader discussions on data protection beyond the elite.

The Mayor insisted on actions beyond dialogues. He cited data misuse examples such as those happening in Uganda where hospitals are sharing patient information without consent, or loan sharks harassing individuals with unwarranted texts. He called for actionable directions and enforcement in such instances that affect personal data and individual privacy. After these remarks, the Mayor officially declared the summit open in the hope that the discussions would lead to transformative actions on data protection in Africa.

The Mayor of Entebbe, Mr. Fabrice Rolinda, welcoming participants to Uganda and to the 2024 DPAS.

DAY ONE: PART TWO

Keynote One: Privacy Enforcement in The Digital Age: Challenges, Solutions & Strategic Partnerships

By Mrs. Drudeisha Madhub – Commissioner of the Data Protection Office, Mauritius

Mrs. Drudeisha Madhub, Commissioner of the Data Protection Office in Mauritius, delivered a keynote speech on 'Privacy Enforcement in the Digital Age: Challenges, Solutions & Strategic Partnerships.' In her keynote, she underscored the significance of data privacy, highlighting its connection to fundamental human rights. She also discussed the challenges in enforcing data protection laws; including resource constraints, human expertise and the complexities of regulating big tech industries. Mrs. Madhub stressed that enforcement is a shared responsibility among regulators, controllers and processors, and emphasised the need for collaboration and strategic partnerships among regulators, regional forums and international organisations to address data protection challenges.

She highlighted the importance of awareness and training programmes for data protection officers and professionals. Additionally, she shared Mauritius' experience in data protection, including its ratification of Convention 108, collaboration with the African Union and efforts to achieve EU adequacy.

Her keynote concluded by emphasising the need for solid foundations in data protection frameworks and the importance of collaboration and strategic partnerships in addressing the challenges of data protection in the digital age.

Panel Discussion

Following the keynote speech, Mrs. Drudeisha Madhub was joined for a panel discussion on the keynote moderated by Dr. Patricia Boshe – Senior Researcher at the University of Passau (Germany), and discussants Ms. Morine Amutorine - the

Africa Sandboxes Forum Lead at the Datasphere Initiative, and Ms. Jenna Franklin - corporate lawyer, trained barrister and senior data protection and privacy specialist (UK), who joined virtually.

Challenges in Enforcing Data Protection in the Digital Era

The moderator began the session by inviting the panellists to share their insights on the challenges of enforcing data protection in the context of digital innovation and emerging technologies.

The discussion emphasised the importance of balancing risk management and enforcement in data protection rights. Panellists acknowledged challenges of governing data in organisations, particularly with emerging technologies like AI, and the challenges in regulating the ever-evolving technologies. Part of the solution discussed by the panel is the importance of adopting a prevention-focused approach and principle-based approach to support the protection of personal data and navigate data management in organizations' processes. Despite legal challenges in regulating technology, the panel advocated for the adoption and implementation of robust privacy frameworks as well as the deployment of awareness programmes to effectively mitigate related risks. This means collaboration between strategic partners within organisations to develop robust frameworks for data protection. Lastly, the panel indicated three key pillars for data governance, namely data protection/privacy, data security and resource (human) management.

Implementing Data Protection through Sandboxes

The panel discussed the role of sandboxes and how they can support data protection authorities or organisations in the effective implementation of data protection within their respective domains. To enable the understanding of what sandboxes for Summit participants are, a clarification was given as 'time-bound, safe and collaborative environments where regulators, innovators and stakeholders can test new technologies and practices against regulatory frameworks.' This means sandboxes can be operational, regulatory or hybrid. Sandboxes support collaborative data protection compliance in an innovative way – for example, collaboration between regulators and innovators. The panel clarified this approach by citing FinTech as one of the most common areas where sandboxes have been used to support compliance. Similarly, sandboxes can be used to experiment and support compliance with other sectors.

Balancing Regulations and Innovation

The discussion shifted to exploring regulation and innovation. The central aim was to implement a balance solution to regulation without stifling innovation, particularly in the context of rapidly evolving technology. The moderator invited the panel to share insights on what approaches would be effective to support innovation whilst ensuring data protection.

The panel stressed the importance of regulation and oversight even though regulatory development may seem redundant in catching up with technological innovation. However, regulating technology should take cognisance of the need to support (tech) innovation rather than stifle it. Sufficient (but not extreme) tech regulation is necessary in upholding individual rights, supporting inclusion (and avoiding bias) and creating a level ground in innovation.

Although some view tech regulation as too onerous, it is necessary to prevent harm and ensure responsible use of technological innovation such as AI. The panel further insisted that, as different countries are adopting various approaches to regulating AI, harmonised standards would be beneficial in elevating compliance and technical requirements.

Leveraging Strategic Partnerships for Effective Data Protection Enforcement

As for strategic partnerships concerning data protection enforcement, the panel underscored the critical role of partnerships and stakeholder engagements in data protection, especially in shaping regulations. Caution was given on regulations developed without broad sectoral consultation as they may yield ineffective or detrimental outcomes. The panel emphasised on the importance of inclusivity and regulatory approaches that take into account local contexts, concerns and enforcement capacities. Public consultation would support people-centric data protection policies, strategies and practices, as well as relevant contextual laws.

Sandboxes and Cross-Border Data Transfer

The panel also explored the use of sandboxes as a tool to facilitate collaboration among data protection authorities, particularly in cross-border data flow cases. Since sandboxes support collaborative enforcement, they can hugely support cross-border enforcement by facilitating collaboration among regulators across different geographical borders. To illustrate this, when setting up a sandbox, regulators can identify issues, set goals and invite stakeholders. Multiple regulators can work together and sandboxes enable this collaboration. While the process can be time-consuming, it's beneficial as it ensures all necessary stakeholders are involved, leading to better regulation and innovation. In addition, sandboxes help identify the right regulators to bring on board and prevent issues that may arise from unregulated data sharing. In principle, the discussion on the use of sandboxes advocated for the use of sandboxes to support and simplify cross-border data protection compliance.

Regulating Emerging Technologies

The moderator wanted to know whether traditional data protection authorities are capable of regulating emerging technologies like AI or there is a need for a new type of regulator for technologies such as AI.

When reflecting, the panel emphasised on the fact that data protection is cross-cutting and intersects with various legal fields, such as intellectual property, competition law and criminal law. To effectively regulate data protection, collaboration with other regulators is crucial. For example, partnerships are necessary for:

- Developing guidelines for the financial sector in collaboration with the Central Bank and other financial entities; or
- Working with the ICT regulator on a Supreme Court case related to SIM card registration and data protection.

This means the current authorities are valid and capable, but would need to collaborate with specific sectors in order to understand specific industry nuances and what they mean in data protection, in order to be able to enforce compliance and develop sector specific regulations or approve codes of conduct. Data protection authorities must work with multiple stakeholders to ensure effective regulation in order to support data protection compliance in a rapidly evolving technological landscape.

Challenges and Solutions regarding Data Protection Enforcement

To wrap up, the panel re-visited some challenging aspects of data protection enforcement in the digital era, as well as proposed solutions. In terms of challenges, the discussion identified the enforcement of data protection laws and insufficient penalties for non-compliance as one of the main challenges. Proposals to overcome the identified challenges included:

- Increased enforcement and monetary penalties.
- Global collaboration to adopt similar regimes and enforcement approaches.
- Cross-border data transfer agreements and adequacy arrangements.

Another challenge worth mentioning is the cross-border enforcement of data protection laws in a continent characterised by a fragmentation of laws, regulations and policies. For example, it was expressed how the lack of legal harmonisation may affect cross-border solutions, like mobile money (like M-Pesa), that operate in multiple African countries. Proposed solutions to such challenges include:

- Cross-border collaboration to harmonise data protection laws and regulations.
- Utilising collaborative spaces like regulatory sandboxes to balance data protection and openness.

Above all, the panel insists on countries' preparedness to counteract negative impacts and consequences of data misuse. At the continental level, (specifically regarding cross-border data protection and compliance) the proposal was for the African Union to develop certification standards for digital technologies and solutions. Introducing such a framework with strong data protection clauses in the certification standards could build credibility in how digital products are marketed and protected across the continent.

Interactive Session

An interactive session followed the panel discussion, and the audience had a chance to contribute to the discussion. The audience wanted to know whether African governments have control over its data; the feasibility of African governments to demand from big tech companies control over data generated by emerging technologies on the continent, considering the current power dynamics, and if regulation is enough to shift power dynamics similar to the EU's approach, taking into account economic and political factors.

In response, the panel stressed the importance of legal and regulatory contextualization, and the fact that the EU model, as good as it may be, cannot be adopted in a copy and paste approach, it must be customised to fit African realities.

In data protection, local standards typically prevail over international ones unless adopted into a national legislation. While global standards are valuable, country-specific regulations are necessary to address actual nuances.

Another question on cross-border data flows was paused with the audience wishing to know if it would be practical to establish a certification agency within the African Union to support continental data flows and data protection. And if so, who should be involved in composing or governing such an agency.

The panel was of the view that a certification mechanism for data protection in Africa, led by the African Union, could help harmonise standards across the region. Like the approach taken by the EU involving certification procedures and mechanisms to support data sharing with third countries. A regional certification mechanism tailored to Africa's needs (like a regional ISO standard) could help support cross-border data flows, reduce data breaches and support the harmonisation of industry practices across Africa.

As for the follow-up question, the audience needed to know whether Africa should develop a unified law for data governance across the continent, rather than having individual countries create their own laws.

It was clarified that states have sovereignty to make laws within their domestic boundaries. However, Africa as a continent can develop (and has developed) a unified approach to support African countries with coming up with their own domestic frameworks for data protection. An approach that the continent has taken is for it to provide an example (a blueprint) which member states can draw from to support continental wide alignment.

The discussion highlighted the challenges in balancing innovation and regulation in data use, particularly when combining non-personal data and personal data that can potentially affect individual identities and hence their rights. To address the challenge of distinguishing between personal and non-personal data, the panel insisted on the role of organisations to implement robust data governance frameworks and utilise technologies that can tag, classify and protect data accordingly. This includes techniques such as pseudonymisation and anonymisation, as well as employing techniques such as tokenisation to secure data. By separating personal data from non-personal data and ensuring proper controls are in place, organisations can mitigate potential risks and comply with data protection regulations.

A question on how public awareness on data protection can be improved was paused. This question was triggered by the concern that many people, unknowingly, share sensitive information online which can lead to the misuse of such data. In response, the panel emphasised on the importance of public awareness and the need for digital education on data protection. It insisted on its crucial role and urged that such education should start from a young age. It noted that awareness and education on data/digital protection must be integrated into the education system from primary to tertiary levels. As an example of best practices, an illustration of Mauritius, where the government, through the data protection office, has taken steps to promote data protection education, including creating booklets and developing an AI-powered educational video for schools, was given.

Lastly, the audience wished to know if the Malabo Convention can support African countries in developing a robust data protection compliance system. The panel repeated the importance of the Malabo Convention. However, like any international document, it requires periodic updates to stay relevant. It needs to be updated to address regulatory development and innovation gaps, and modernised to effectively protect personal data across the African continent.

The Panel: *From left to right: Dr. Patricia Boshe – Senior Researcher at the University of Passau (Germany), Mrs. Drudeisha Madhub – Commissioner of the Data Protection Office of Mauritius and discussant Ms. Morine Amutorine – the Africa Sandboxes Forum Lead at the Datasphere Initiative.*

DAY ONE: PART THREE

Keynote Two: People Empowerment in Data Protection and Privacy: Fostering Transparency and Trust in Digital Service Delivery

By Mrs. Stella Alibateese - National Director of the Uganda Personal Data Protection Office

The keynote of Mrs. Stella Alibateese, the National Director of the Personal Data Protection Office (PDPO) narrated the importance of people empowerment in data protection and privacy, and fostering transparency and trust in digital services in Africa. She made a reference to the objectives of the African Union Digital Transformation Strategy (2020-2030) concerning the need to secure Africa's digital single market by 2030. She acknowledged that while digitisation in Africa brings opportunities, there are also challenges like privacy concerns, data harvesting and cybercrimes. She emphasised that data protection laws, such as Uganda's Data Protection and Privacy Act, are crucial for empowering data subjects and building trust through transparency and compliance. She added that key principles like accountability, lawfulness and transparency in data processing are essential, and that data breaches can be reduced by training staff and implementing technical aspects such as privacy by design.

She further noted that independent data protection authorities are important for enforcement, and as an example, she referenced Uganda where penalties for non-compliance can include fines of up to 2% of annual gross turnover and imprisonment. She stressed that balancing digitisation benefits and data privacy risks would ensure that data subjects' rights are respected.

Panel Discussion

To dig further into Mrs. Alibateese's keynote, Ms. Teki Akuetteh, Executive Director of the ADRH, called for a panel discussion composed of Mr. Maxence Melo –

Executive Director of JamiiForums (Tanzania), Mr. Matthew Martin – CEO of Two Candlesticks (U.S.A), Ms. Jackie Kitiibwa - Digital Economy Lead at FSD (Uganda) and Mrs. Stella Alibateese - The National Director of the Personal Data Protection Office (Uganda).

People Empowerment in Data Protection and Privacy: Fostering Transparency and Trust in Digital Service Delivery

The moderator re-introduced the keynote topic, acknowledged the importance of digital services in Africa and invited the panel to share their thoughts on the topic. The discussion began with the conversation on digital rights and data privacy with the panellists insisting on the need to advocate for data protection frameworks to support individual rights and citizens' ability to exercise their civic rights in the digital sphere. An example was shared which related to how some communities on the continent were sceptical to adopt such frameworks but eventually they recognised their importance. The realisation was only possible after communities were made aware of the importance of safeguarding personal data. In an example from Tanzania, citizen awareness was facilitated through online education using an online platform where people can access different tools and engage in discussions – freely and in whatever language of their choice. Caution was given on the fact that online platforms can simplify public awareness and support a wider outreach, but it can easily be manipulated through mis/disinformation and therefore, there is need for information control, moderation and fact-checking. There are also other risks that need to be considered such as cybercrime and misuse of data.

Another example on people empowerment was given and it concerned the use of universal inclusive approaches that are transparent and user-friendly. These could support people empowerment by safeguarding their rights – including their data protection and privacy rights. Such standards, when set up and implemented in a transparent manner, invoke people involvement. To illustrate this fact, a reference was made to a 2021 study on digital financial services, which revealed significant gaps in data protection and transparency. The study analysed terms and conditions across four industry verticals (mobile betting, e-commerce, mobile banking and ride-hailing) and found a lack of standardisation, inconsistent language and inadequate information on data storage and usage. The key findings included:

- Regulatory gaps in enforcing data protection standards
- Business priorities over data privacy concerns
- Lack of embedment of data protection by design in business models.

The panellists emphasised that empowerment requires the understanding of customers' situations and deliverance of value to them, while, at the same time, safeguarding their rights. The unified message on people empowerment concerned the importance of education and awareness programmes. To achieve this, businesses were reminded about their role to support awareness which would consequently support their companies in compliance. Companies should view data protection as a business differentiator driven by consumer demand.

Empowering and involving creates a trusting relationship. Trust in a business is a multifaceted aspect that needs to be viewed and approached holistically. Trust encompasses not only data protection but customer involvement and understanding of business processes, (promoted through transparent practices) and effective crisis management. This underscores the importance of building trust through transparent and responsible business practices, and effective responses to problems.

Approaches to Fostering Transparency and Trust

The moderator extended the discussion on the importance of trust in business, particularly in relation to data protection. She noted that companies that recover well from mistakes can emerge more trustworthy. She noted there is a substantial increase in data breaches involving personally identifiable information. In a concerning tone, she posed a question to the panel on whether current approaches to data protection support sufficient transparency and trust, or there is a need for new strategies. As a way of seeking solutions, she wondered whether we should still focus on rapid recovery from breaches or shift to empowering individuals and take a more active role in protecting their personal data.

In response to these questions, the panel acknowledged the complexity of the question but was not so much surprised by the increase in data breaches given the prevalence of human interaction in business services and the use of technology. However, the panel was of the view that more can be done, particularly in the African context where countries are at varying levels of development in data protection. For example, Mauritius has 18 years of experience, while Uganda has 3 years of experience with data protection enforcement. This means a high level of collaboration and coordination among regulators is inevitable to deal with such incidences but also to create public trust in the safety and protection of personal data across the continent. In addition, data protection affects multiple sectors, therefore, both vertical and horizontal coordination and collaboration is crucial.

There is a need for data protection authorities to collaborate not just amongst themselves, but also with other regulators such as those overseeing the financial sector and health clinics. There is a need to build on existing frameworks and work together to make meaningful progress in data protection.

Public Awareness and Digital Services Delivery

To expand on the discussion on public awareness, the moderator asked the panel to share their perspectives on the current state of awareness regarding digital services delivery and the roles that governments, civil society and industries should play in empowering individuals in this area.

Once again, the panel was unified on the importance of public awareness. However, in the context of the question posed, the panel focused on awareness by data controllers and data processors – especially regarding the use of online platforms to share personal data. An example that was given concerned a popular practice in Tanzania where Masters of Ceremonies (MCs) in events such as weddings would take pictures and film videos, and share such information on their personal or business social media platforms. These acts are done in ignorance of the data protection rights of individuals attending such events, as well as the duties of data controllers and data processors. Addressing such practices requires a nuanced approach, starting with awareness-building rather than punitive measures. In cases involving institutions, an approach taken by the South African Information Regulator can be taken. The South African Information Regulator has taken an approach consisting of issuing statements when institutions or state actors violate data protection. These send a strong message to the public on reporting data violations. They also give the public a cue on their right to report violations.

Regarding the duty to raise public awareness, one of the panellists noted and commended Tanzania's Personal Data Protection Commission for conducting awareness campaigns for both the public and state actors who collect and process data. The Commission uses citizen-centric approaches with the aim of empowering. This is because citizens, who are primary data subjects, often do not know their rights, especially in vulnerable situations.

Responsibility of Protecting Personal Data

The discussion turned to the question of responsibility regarding protecting personal data. The moderator noted that laws place responsibility on businesses to protect personal data and wanted to get the panel's opinion on whether relying solely on businesses to protect personal data is ideal or there should be a shared responsibility among all involved stakeholders.

A panellist leaned on the need for shared responsibilities in protecting personal data. Different stakeholders have different roles to play. For example, governments have a role in educating citizens about their rights and potential dangers of data breaches. Governments adopt creative approaches such as ones adopted by institutions like the National Park Service, which developed the "Don't Pet the Fluffy Cows" campaign and used social media to raise awareness and change behaviour. To roll out such campaigns, governments can utilise social media and influencers to communicate the risks associated with data processes and how one can participate in protecting their personal data and react in cases of data breaches. On the other hand, businesses should focus on educating consumers about how they handle data and the benefits of sharing data, and supporting consumer trust. By doing so, consumers can make informed decisions about sharing their data, weighing the benefits and risks.

In general, governments are best positioned to communicate risks and rights to citizens in a neutral manner, although businesses can support data protection by prioritising transparency and building trust with their customers.

Data Protection Terms and Conditions

The panel concluded with a discussion on a controversial topic: data protection terms and conditions. These are usually published on websites in length and contain complex legal language that is not easily understood. The question was whether individuals in the informal sector understand or review the terms and conditions they agree to, and what steps civil society organisations are taking (can take) to address this issue. The question was answered using research conducted by FSD on consumer comprehension of terms and conditions across different platforms, including smartphones, feature phones, USSD and SMS. The research revealed significant variations in comprehension and led to recommendations for regulators. The recommendations included the need to develop concise critical information summaries highlighting key risks and exposures associated with digital platforms. Also, CSOs could, just like how FSD works in collaboration with the UK Information Commission to develop toolkits for compliance, work with data protection commissioners to support compliance through, for example preparing simplified e-consent solutions.

Final Remarks

The moderator concluded the panel session by inviting each panellist to share their final thoughts. Key takeaways included the following:

- Empowering people is crucial for effective data protection, and stakeholders should take measures to empower individuals to protect their data.
- Collaboration is essential for data protection, both locally and internationally, and stakeholders should work together beyond conferences to safeguard individuals' rights.
- Education is vital for data protection, and regulators, government agencies and non-profit organisations should focus on educating the public on safe internet practices, including responsible data sharing.
- Effective feedback mechanisms between regulators and industries are necessary, given the rapidly evolving nature tech that facilitates data processing. Ongoing collaboration is key to refining respective sector-specific policies and practices.

Interactive Session

The closing of the panel discussion was the opening of an interactive session and the audience actively engaged with questions and comments. Three questions were paused:

1. Should government entities and telecom companies in Uganda be held accountable for protecting citizens' data and preventing identity theft?
2. How can financial institutions and mobile telecom companies ensure the security and compliance of client data in collaborations, especially when data is transferred across borders, to maintain transparency and trust?
3. Could fiduciary obligations, like those concerning the banking sector, as opposed to consent-based frameworks, offer a more effective approach to regulating data collection and ensuring that data handlers act in good faith? [Since consent-based data protection frameworks have been criticised for being ineffective as individuals may not fully understand the nature of consent clauses and risks associated with data use.]

In response, the panel reiterated the obligation government entities have in protecting personal data. Like any other data controller, government entities are accountable for their processing of personal data, and the Data Protection and Privacy Act of Uganda applies to the public sector as well. In cases where compliance is challenging, the Personal Data Protection Office works to support government ministries to ensure compliance, especially for high-risk projects. However, individuals also have a role in protecting their data. For example, when using services like mobile money, users must safeguard their PINs and sensitive information.

For the second question, the panel explained that laws would usually provide rules on sharing or storing personal data outside the country, and organisations are expected to comply. However, empowering users is crucial, and education on data protection should go beyond technology and businesses to include individuals.

Lastly, the panel insisted that consent is not the only lawful basis for collecting and processing personal data; other lawful bases may apply. Guidance on determining a lawful basis for data collection is essential for organisations and for individuals to know.

Data Protection Compliance: A Catalyst for Africa's Digital Transformation
PARTNERS
Meta

The Panel: *From left to right: Ms. Teki Akuetteh – Executive Director of the ADRH, Mrs. Stella Alibateese – The National Director of the Personal Data Protection Office (Uganda), Mr. Maxence Melo – Executive Director of JamiiForums (Tanzania), Mr. Matthew Martin – CEO of Two Candlesticks (U.S.A), and Ms. Jackie Kitiibwa - Digital Economy Lead at FSD (Uganda).*

DAY TWO: PART ONE

Day two of the event started right away with the introduction of speakers and thereafter, the keynote speech. The day consisted of two keynote speeches, panel discussions, Q&A sessions and a closing ceremony. The closing ceremony entailed a special performance, acknowledgments and appreciations, closing remarks and the unveiling of the venue for the next Data Protection Africa Summit.

Keynote One: Leveraging Data for Competitive Advantage: Striking a Balance between Business Needs and Regulatory Compliance

By Mr. Steve Wood - Director and Founder of Privacy X Consultancy and a visiting policy fellow at the Oxford Internet Institute

Mr. Steve Wood, the Director and Founder of Privacy X Consultancy, and a visiting policy fellow at the Oxford Internet Institute, delivered a keynote address for the first session of the second day of the summit. His keynote speech focused on how new technologies are driving demand for data across the so-called fourth Industrial Revolution which is basically a fusion of technologies i.e. AI, IoT, the cloud and the entire combination of these technologies which creates this new industrial revolution. This revolution creates new opportunities to support economic growth. If we think about AI, the GSMA, the international body representing mobile network operators, has estimated that AI could increase Africa's economic growth by 2.9 trillion dollars by 2030. However, while reaping these benefits and supporting the fourth industrial revolution, there is the need to ensure data is used responsibly to support innovation and comply with regulatory requirements.

It all boils down to data innovation. The concept which he narrowed down into two concepts; data discovery and data application, which are characterised as thinking with data and acting with data. An approach to accountability that can enable us to understand risks of data innovation and how we should build accountability programmes around that. The two concepts help us think about where the risks and harms are most likely to happen, and where we should particularly think about building the safeguards in relation to responsible data innovation.

According to Steve, data discovery is about the research into innovation in terms of developing different applications and systems that may use personal data, but does not have a direct impact on individuals as it is deemed as the piloting phase, while data application involves acting with the data that has been collected and this has a direct impact on the data subject.

Steve emphasised that it is important to think about these two concepts as it helps identify where the risks and harms are most likely to manifest, and where safeguards must be built towards responsible data innovation.

He then highlighted how personal data may be leveraged in Africa for competitive advantage and for innovation and growth of digital products and services. An example of such is how personal data is used in personalised services online – using data to tailor content to individual needs to drive personalised services which can deliver extra value to organisations. How data is used to support service delivery is the engine of the fourth revolution.

It is very important to understand the harms and risks that can occur in leveraging personal data to support digital products and services. To have a sophisticated approach towards understanding these harms in order to curb them is crucial. In explaining this, he referred to the harm taxonomy of the UK Information Commissioner's Office which breaks down the different types of harm that can occur from particular uses of personal data in offering products and services. These harms include financial harm, physical harm and psychological harm. And of course, the nature of the harm depends on the different types of personal data processing; varying levels of harm means varying levels of likelihood.

This means the responsibility of organisations in harnessing the opportunity to use data for innovations and digital products and services is to have sophisticated ways of understanding the potential harms and then think about how they can mitigate these harms. He added that the presence of these harms should not prevent organisations from innovating. Rather, organisations must have a clear audit trail to make sure they can demonstrate how they mitigate harms and risks, and that the risks of these harms occurring have been reduced either completely, to an acceptable level low enough that they no longer present a real danger to individuals.

In addition, Steve shared with the audience one of the key tools to help us understand the opportunities and benefits alongside the harms that can occur from using personal data. This is the data protection impact assessment. He noted that many data protection laws in Africa have provisions on conducting data protection impact assessments. He emphasised on the importance of equipping organisations that want to innovate with personal data and with the skills to be able to effectively implement data protection impact assessments to enable staff to understand how to actually map the different types of personal data flows. This is crucial for when organisations intend to roll out new products, services and innovations. Understanding how a data protection impact assessment is conducted will also help staff to understand data and know how to actually map the different types of risks and harms, and document them.

Another tool to support the use of data in an innovative context is data protection by design and by privacy-enhancing technology. This will enable organisations to consider different solutions that can minimise the amount of personal data used for innovation – such as by pseudonymising or anonymising personal data, or minimising the amount of personal data that is shared between different third parties who are involved in a data sharing aspect of the product and service.

He concluded with a thought-provoking contribution; whether (and when) organisations should rely on digital consent or other lawful bases to process personal data. There are instances where the need for data subjects to control their data outweighs public interest. In such instances, organisations can rely on digital consent. However, there are instances where organisations need to use personal data for public interest, for example, to conduct health research and the need to have access to a wider population of data. Organisations can use legal bases provided in data protection laws relating to legitimate interests. Legitimate interests enable an organisation to demonstrate the necessity and legitimacy of using personal data to address an important aim, and that aim may be in public interest.

Panel Discussion

To debunk points advanced by Mr. Wood in his keynote speech, the session moderator Mr. Kwaku Nhyira-Addo invited three experts, Dr. Ernest Mwebaze - Computer science and machine learning expert, and a co-founder of the Makerere University AI lab (Uganda); Mr. Dickson Katto - Head of Data and Commercialisation at Stanbic Bank (Uganda); and Mrs. Barbara Among Arinda (Uganda) to a panel discussion.

Leveraging Data for Competitive Advantage

The moderator started the session by asking how regulators and organisations can harness data collected and stay within regulatory green zones.

The panel began the discussion by indicating the inevitable need for organisations to understand business priorities at any given time and then align their data strategy. The panel emphasised that risks associated with leveraging data for competitive advantage must be minimised by collecting the right data for a specific use (purpose limitation and data minimisation). Data collection must be done responsibly to protect consumers' personal data while supporting trust.

Implementing a Robust Data Governance Accountability Framework

After this, the moderator asked about implementation of a robust data governance framework which ensures consumer protection from the never-ending appetite for profit of businesses. The panel noted that in order to ensure the highest measure of accountability, businesses must be aware of and acknowledge consumer rights which are enshrined in different data protection laws across Africa.

The moderator wanted to know how businesses could maintain protected access to personal data and ethical business practices. In response, the panel remained vigilant on the need for businesses to stay ethical while processing personal data for the benefit of the business. It insisted on having an internal policy framework that guides the business (data governance and management) using the core regulatory framework. And this should be implemented across businesses, especially where a business is operating in different countries.

The panel added an important aspect, namely corporate social responsibility. Organisations need to identify their social responsibilities which can also support consumer trust even in the absence of regulatory frameworks. To do this, businesses must take a holistic approach that goes beyond inward looking (focus on growing profits and revenue) and consider external factors such as consumer needs and protection. Customers will be willing to support innovation if they can see how they can benefit and how their rights can be protected.

Additionally, the panel emphasised the need for regulators to be more agile and flexible. As regulations and policies may not be able to catch up with tech innovation such as AI, regulators must come in to harmonise this regulatory gap whenever necessary. Furthermore, research is necessary and important to understand product development (and service provision) which goes hand-in-hand with legal compliance (compliance by design). To conclude, the panel emphasised the need for regulators to adopt a hybrid but localised approach to regulation while looking at the future of respective industries, in order to support innovation and regulatory flexibility.

Interactive Session

Following the panel discussion, the session transitioned into an interactive question and answer session where the audience was welcomed to ask questions or contribute to the discussion with a comment.

The first question concerned the need to understand what businesses are doing to limit or mitigate the risks of harm associated with data collection. In response, the panel explained that every organisation is expected to ensure that data is protected at all stages through effective organisational and technical measures. Such measures must be continuously monitored and improved. It was emphasised that businesses hold a core responsibility to remain transparent and act swiftly in reporting data breaches to appropriate authorities. Such accountability, the panel noted, is critical in mitigating risks linked to data collection and maintaining public trust.

Another participant asked how organisations across Africa can effectively manage cultural, digital and regulatory changes while promoting data literacy and compliance. The panel acknowledged that there is a growing digital divide which risks leaving behind communities without access to technology. They emphasised that before conversations about data protection and literacy can be meaningful, basic infrastructure such as electricity must be provided. Furthermore, regulatory authorities were urged to ensure protection for vulnerable groups, even in cases where individuals may not have direct access to digital services.

Finally, a participant wanted to know whether guidelines could be developed to balance the need for businesses to request and share customer data, and minimise the stress placed on consumers. The panel explained that organisations must have internal policies and conduct data protection impact assessments for risky processes. These, together with data protection principles, should provide a foundation that supports organisations' activities and reduces the burden for consumers tied to the use of their personal data – if any. The panel further highlighted that data sharing must create shared value, with consumers fully informed of the benefits and giving their consent or understanding legal bases for using their personal data. This is essential for unlocking opportunities in data-driven services while safeguarding consumer rights.

In closing, the moderator stated that the key takeaways are that businesses must operate within the framework of compliance and collaborate in the most efficient and transparent manner because the future is about trust, and that if this kind of collaboration and trust exists, both customers and businesses win.

The Panel: *From left to right: Mr. Kwaku Nhyira-Addo – a broadcast journalist, branding and communications consultant, and the MC for the DPAS (Ghana), Dr. Ernest Mwebaze – Computer science and machine learning expert, and a co-founder of the Makerere University AI lab (Uganda), Mrs. Barbara Among Arinda (Uganda), and Mr. Dickson Katto – Head of Data and Commercialisation at Stanbic Bank (Uganda).*

DAY TWO: PART TWO

Keynote Two: Unlocking Innovation for Agile Privacy Compliance

By Michael Mulquin - Chair of the Smart Cities Systems Committee of the International Electrotechnical Commission (IEC) and Co-Chair of the IEC/ISO/ITU Joint Smart Cities Task Force

The keynote centred on the critical role of innovation in achieving agile privacy compliance and creating value in data while placing individuals at the heart of data governance. Mr. Mulquin began by highlighting that data protection is not simply a compliance requirement, but a foundational pillar for Africa's digital transformation. He described personal data as a valuable asset, comparing it to gold, and called on stakeholders to act as guardians against misuse, just like James Bond defeating modern day data thieves.

He introduced practical and forward-thinking approaches that can give people greater control over their personal data. These included Personal Online Data Stores, which allow individuals to manage their own information. He also talked about the development of personal data intermediaries and AI-powered mobile assistants that can help users interact with services securely without oversharing their data. Drawing on global examples, Mr. Mulquin showcased Helsinki's proactive public service model where city departments securely share data to offer eligible citizens services such as free childcare or health interventions. He also highlighted IKEA's transparent data-sharing model which builds trust by letting customers decide what data to share in exchange for value-added services.

He stressed the need for governments, regulators and innovators to collaborate using standardised frameworks, such as the minimal interoperability mechanisms recently adopted by the International Telecommunication Union. These frameworks, he said, provide a structured way for communities and institutions to manage personal data responsibly.

Mr. Mulquin closed his keynote speech by challenging the audience to become the "James and Jane Bonds" of data protection within their respective sectors. He called for bold leadership from regulators, city authorities, businesses and technologists in order to unlock innovation, build trust and return control of data to the people it belongs to.

Panel Discussion

The panel discussion that followed the keynote, "Unlocking Innovation for Agile Privacy Compliance" brought together a range of professionals from the regulatory, technology and data governance sectors. The conversation focused on what agile privacy means in practice, how organisations are adapting and the central role of people and technology in enabling responsive and inclusive data protection systems.

To begin, the panel unpacked the concept of agile privacy. They noted the absence of a single textbook definition but agreed that agility in privacy programmes means having the structure to support flexibility, being responsive to regulatory changes and adapting to technological developments. Agility also involves embedding privacy into product development cycles and allowing organisations to remain compliant while innovating. The panel stressed the importance of breaking down privacy efforts into manageable phases, or "sprints," to support measurable and iterative progress.

The discussion then turned to the role of technology. The panel highlighted that while technology can streamline privacy compliance and enhance collaboration across teams, it must be applied thoughtfully and in context. For smaller organisations, the cost of high-end privacy tools can be prohibitive. Therefore, scalable and open-source solutions were seen as valuable options. Ultimately, technology should not be adopted for its own sake, but to solve clearly defined challenges and improve how data is governed. When asked about tools that can support agile practices in real time, the panel offered practical examples, such as privacy dashboards, data tagging and permission tracking mechanisms. These tools can help organisations manage personal data across its life cycle and ensure accountability when data is reused or shared across departments or services.

The importance of collaboration was another recurring theme. The panel emphasised that privacy is not the sole responsibility of legal or compliance teams. They require coordination across product development, engineering, the law and leadership. Organisations need governance structures that support cross-functional engagement and mechanisms for early consultation during product design.

On the people front, the panel agreed that training and awareness are essential. Organisations must invest in role-based training and continuous education to ensure that all staff, regardless of function, understand how privacy applies to their work. Several strategies were discussed, including appointing privacy champions within teams and integrating privacy into agile development sprints. To ensure accountability and scalability, some organisations have implemented structured governance models centred on risk assessment, compliance and governance. These models help align business objectives with privacy commitments and they involve internal collaboration, regular privacy reviews and automated triggers within development workflows.

The session concluded with a call to keep community and end-user needs at the heart of business efforts. The panel encouraged participants to pilot new approaches, seek feedback and build data privacy programmes that reflect the realities of users especially in African contexts where access to digital tools may vary widely.

Interactive Session

Following the panel discussion, the session transitioned into an engaging question and answer session. Participants raised thoughtful questions on community involvement, digital identity systems, data control and the responsibilities of different actors in managing data privacy risks.

First of all, a participant wanted to know how digital innovation efforts can meaningfully include communities, especially those often left behind in technology rollouts. The panel acknowledged that while innovation and technology are important, real transformation only happens when communities are involved from the start. They emphasised that effective tech innovation must take into account the real-world conditions of people who may not have access to smartphones or internet-based platforms. Community input was highlighted as a critical success factor.

The discussion also addressed the growing use of digital identity systems, where users can log in to one platform using credentials from another. A participant raised concerns about the trust in such systems, noting that while one platform may accept identity data from another, the reverse is not always possible. The panel recognised the convenience offered by these systems but cautioned that they come with added privacy complexities. Users often grant access to multiple third parties without fully understanding the extent of data sharing and security risks. The panel stressed the importance of user education and transparency, while also recognising that companies and regulators have shared responsibility in managing associated risks in such practices. On the issue of who is ultimately responsible for assessing the risks in data-sharing partnerships, the panel concluded that responsibility is shared. Companies are required to be transparent and provide tools for users to manage their data. At the same time, users must engage with the tools provided and make informed choices. Regulators play a critical role in ensuring accountability across the board.

Throughout the discussion, the panel reiterated that privacy programmes must be adaptable, user-focused and inclusive. The theme of agility remained central as participants were reminded that privacy frameworks must evolve alongside technological change.

Data Protection Compliance:
A Catalyst for Africa's Digital Transformation
PARTNERS
Personal DATA Protection OFFICE
Hewlett Foundation
Meta
Internet Society
ESTICKS

The Panel: *From left to right: Michael Mulquin – Chair of the Smart Cities Systems Committee of the International Electrotechnical Commission (IEC) and Co-Chair of the IEC/ISO/ITU Joint Smart Cities Task Force, Dr. Ololade Shyllon, head of Privacy Policy across Africa, the Middle East and Turkey (AMET) for Meta, Ms. Teki Akuetteh – Executive Director of the ADRH, and Mr. Ridwan Oloyede – Director at the Centre for Law and Innovation and the co-founder of Tech Hive Advisory Africa*

Closing Ceremony

The three days full of learning and networking during the 2024 Data Protection Africa Summit ended with a memorable conclusion. First, the MC Mr. Kwaku Nhyira-Addo expressed deep appreciation to all who attended the DPAS (participants, presenters and panellists) for their active engagement, insightful contributions and commitment to advancing data protection across Africa. He reflected on the year's theme which explored strategic partnerships, people empowerment, compliance enforcement and innovation as pillars for Africa's digital transformation.

He recognised the contributions of sponsors, including the Personal Data Protection Office of Uganda, the William and Flora Hewlett Foundation, Meta, the Africa Digital Rights Hub, Nsiah Akuetteh & Co, JamiiForums, the Internet Society, Two Candlesticks and Vincsys whose support made the event possible. Special acknowledgments were given to representatives from various African data protection authorities, with Uganda being highly praised for its role as a gracious and engaged host.

Ms. Teki Akuetteh, Founder and Executive Director of the Africa Digital Rights Hub, delivered an important announcement. She introduced a new partnership between the DPAS and the Data Protection Africa PICCASO Awards, set to debut in 2025. The awards will celebrate African excellence in privacy and data protection, recognising individuals and organisations that are shaping the future of data protection and governance. Ms. Akuetteh explained that "PICCASO" stands for Privacy, Infosec, Culture, Change Awareness and Societal Organisation, emphasising the initiative's focus on fostering a privacy-first mindset.

Mr. Alexander Kiban Dama, Chairperson of the Board of Directors of the National Information Technology Authority in Uganda, delivered the official closing remarks. He commended the collaborative spirit that characterised the Summit, highlighting discussions on harmonising regulatory frameworks, building capacities and raising public awareness. He expressed gratitude to the keynote speakers. Mr.

Kiban Dama encouraged continued collaboration between data protection offices across the continent and expressed optimism about Uganda's potential to lead in data protection innovations.

The organising team from the Africa Digital Rights Hub (ADRH) and the Personal Data Protection Office (PDPO) of Uganda were commended for their unwavering efforts in putting together the event. Team members were individually acknowledged for their behind-the-scenes efforts in planning, coordination and execution - from programme development and communications to logistics and technical support.

Finally, Ms. Akuetteh revealed the venue for the 2025 DPAS edition. She also took this moment to honour long-standing DPAS partners such as the Hewlett Foundation, Meta and other collaborators whose sustained support has enabled the summit's growth over the years. The closing moments encouraged continued networking among participants. The 2024 edition was widely regarded as a successful and impactful gathering, setting the stage for even greater collaboration in the years to come.

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY

Data Protection Compliance:
A Catalyst for Africa Digital Transformation

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY

PHOTOS OF THE 2024 DPAS CLOSING CEREMONY

DAY FOUR: HOST COUNTRY TOUR

The final day of the summit was designated as the Host Country Tour where participants had an opportunity to experience Uganda beyond the conference halls.

Delegates visited the source of the River Nile, one of Africa's most iconic landmarks, and explored the Railway Museum in Jinja Town. The tour offered a blend of cultural enrichment and historical insight, leaving participants with lasting memories of Uganda's natural landscape and heritage.

WELCOME TO
THE UGANDA RAILWAY
MUSEUM
OPEN FROM
AM TO PM
CLASS
PLEASE
SUPERVISE
CHILDREN

RACE
COLONIAL EXPANSION
1931
28

THE "LUN