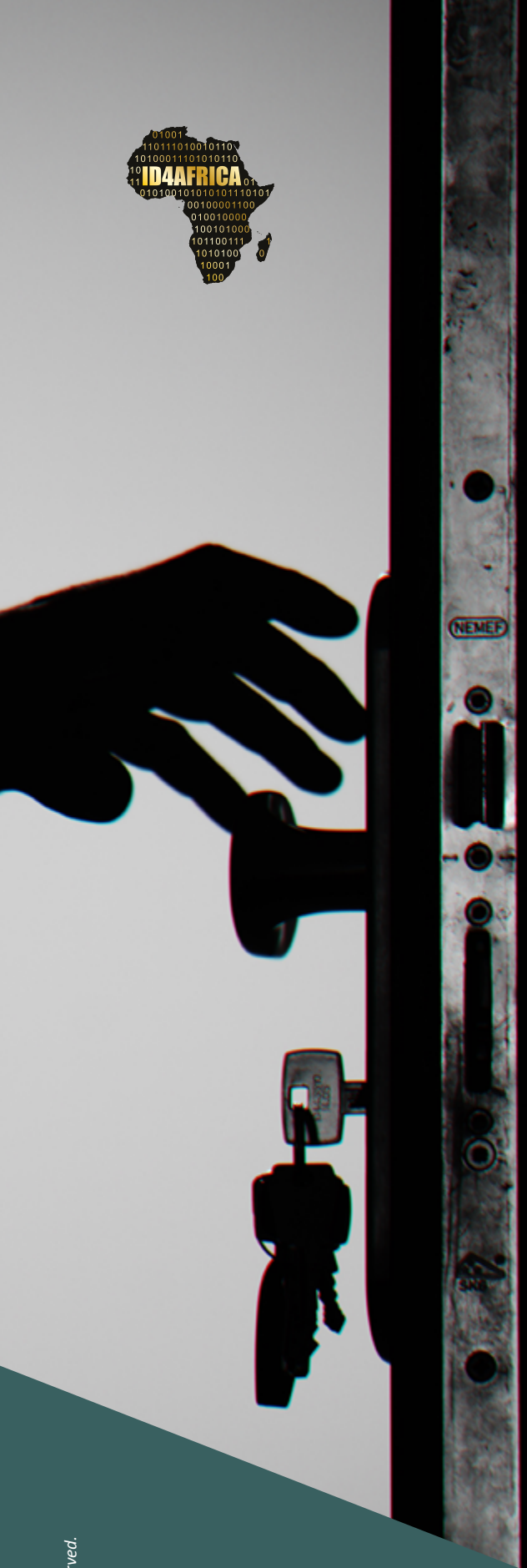


ROUNDTABLE OF AFRICAN DATA PROTECTION AUTHORITIES

Status and response to privacy risks in identity systems

PROCEEDINGS OF A WORKSHOP

PAM DIXON, RAPPORTEUR

Roundtable of African Data Protection Authorities on the topic of privacy and identity systems

ID4AFRICA
5TH ANNUAL CONFERENCE
JUNE 18, 2019

I. INTRODUCTION AND BACKGROUND

The Roundtable of African Data Protection Authorities (RADPA), was held 18 June, 2019 in Johannesburg, South Africa. It was an historic first meeting of the African DPAs to address systemic privacy and data protection risks in identity systems. The meeting was convened by ID4Africa, which is chaired by Dr. Joseph Atick. The workshop was moderated by Teki Akuetteh Falconer, Founder & Executive Director of Africa Digital Rights' Hub and was conducted under Chatham House Rules to facilitate an open exchange. The Rapporteur for the meeting was Pam Dixon, Founder & Executive Director of the World Privacy Forum. Over 40 invited observers from the African and International data protection community also attended the meeting.

RADPA brought together Data Protection Authorities and country level experts to discuss risks, challenges, and potential steps forward to address the risks to privacy in identity systems. To accomplish this, the workshop examined key overall challenges pertaining to privacy, data protection, identity systems and data in Africa, and explored the approaches the represented African countries were using to solve problems in their varying settings. Invited presenters from 10 African countries — either Data Protection Authorities or other country level experts — provided specific case studies of privacy and identity within their jurisdictional context.

The invited DPAs and country level experts further explored and compared experiences regarding the kinds of challenges they were experiencing, as well as opportunities for harmonization of their efforts and discussions of differences in the DPA's statutory mandates and structural compositions. Invited experts shared perspectives on effective enforcement, communication to the public, and working with government officials to promote privacy in identity systems. Participants concluded the meeting by sharing ideas for a path forward and next steps.

Workshop Statement of Task

The objective of RADPA is to facilitate a dialogue among the African DPAs and their allies on Privacy and Data Protection, and the appropriate uses of identity systems and identity data in Africa, and to allow the authorities to network and coordinate their positions on this important matter.

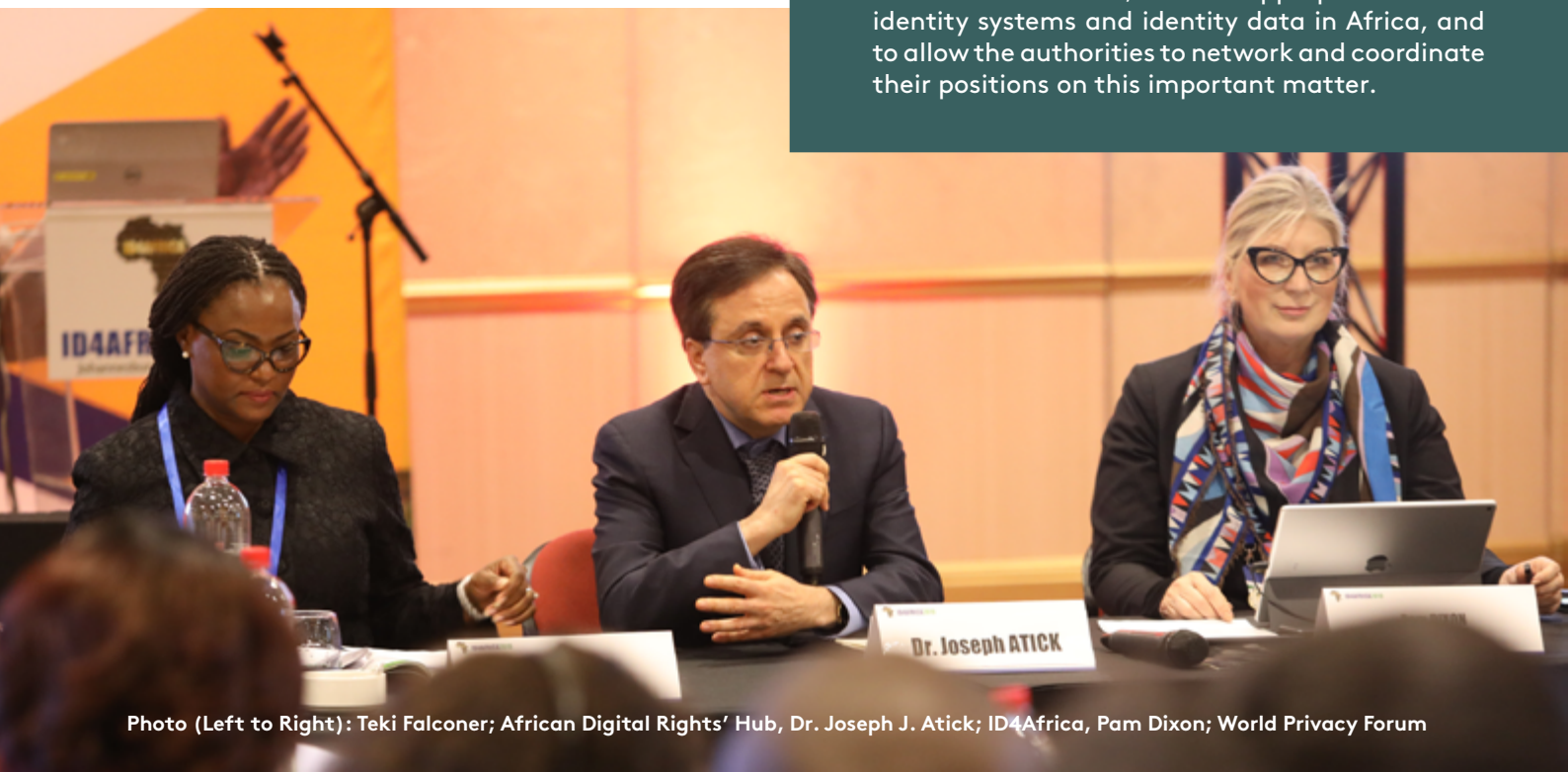


Photo (Left to Right): Teki Falconer; African Digital Rights' Hub, Dr. Joseph J. Atick; ID4Africa, Pam Dixon; World Privacy Forum

II. COUNTRY LEVEL PRESENTATIONS

Highlights from presentations of Data Protection Authorities and country level speakers

- **African countries are passing data protection laws at an increasingly faster rate in the last 20 years.**
- **There is increasing awareness of privacy issues in African jurisdictions, for example, Data Protection Authorities note increases in privacy complaints of 20-30 percent in the past few years.**
- **Although the African countries have varying approaches to the structure of data protection authorities, most structures prioritize independence and allow for a variety of enforcement mechanisms.**
- **Many of the data protection authorities have worked closely on identity systems within their countries, and have either set up national registries or are tasked with authority for enforcing the privacy of those systems. Presenters discussed the high risks of sensitive identity data, and discussed the role of biometrics in identity systems and the need for resources for managing biometric data properly. Some presenters expressed concern regarding the sale of information in identity systems.**
- **The presenters discussed the need for harmonizing privacy principles across African jurisdictions, as well as internationally. Europe's GDPR was discussed as a major impetus for encouraging harmonization of African country-level data protection laws with EU principles.**

The meeting began with opening presentations from country level experts. The charge to the speakers from South Africa, Burkina Faso, Cape Verde, Cote d'Ivoire, Ghana, Kenya, Mauritius, Morocco, Uganda, and Senegal was to provide a concise summary of the most important challenges and lessons from their country that could contribute to advancing collective knowledge about data protection in Africa, with a particular view to identity systems. Experiences, concerns, priorities, goals, obstacles, opportunities, and other issues of central concern were requested for inclusion in the country-level summaries.

The case studies revealed highly varying jurisdictional approaches to data protection, however, there was a unified concern about the sensitivity of identity systems.

During the discussion, experts noted a wide range of implementation dates of country level data protection legislation. The earliest enacted data protection legislation among those present dated from 1993, and the most recently enacted data protection legislation dated from 2019. Enactments in 2001, 2008, 2010, and 2016 are exemplars of the heightened trend in the last two decades for passage of data protection legislation in African countries, with an increase of adoption in the last 10 years.

The structure of data protection authority implementation within the government varies substantively between the countries. While most of the data protection authorities had independent authority, some had dual mandates, or were part of another agency. There were a few core models that emerged from the case studies. One of the most frequently occurring model was that of a commission. Data Protection Commission members in African jurisdictions currently range from as few as 3 to as many as 11. Some commissions had jurisdiction over public and private sectors, but there was variability on this point. Not all countries in Africa have appointed data protection authorities, even if there is data protection legislation, as some jurisdictions do not have this requirement. Some but not all jurisdictions provide for the constitutional right to privacy.

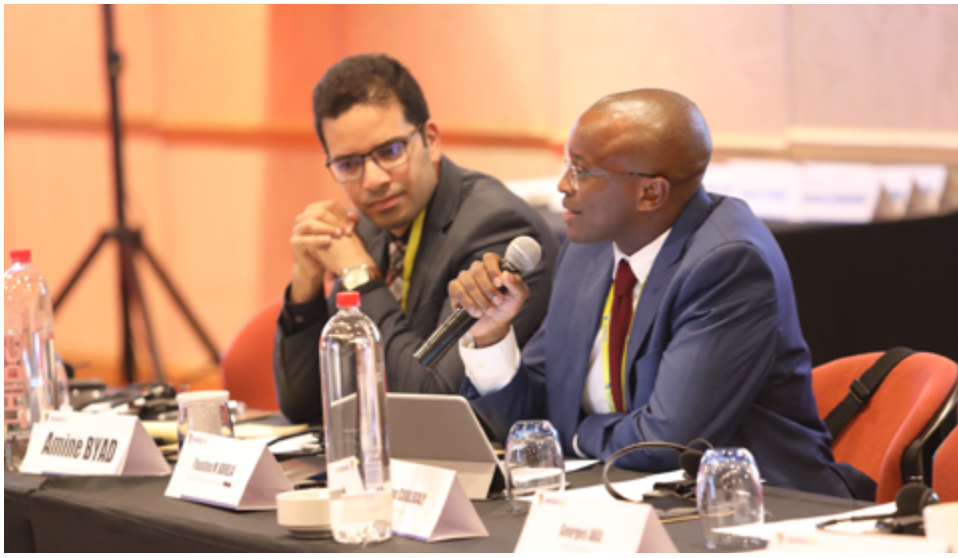
A theme among the case studies was the issue of sensitizing their constituencies to data protection and privacy, and the importance of addressing the concerns of young people. Several presenters noted that the majority of people working in the data protection field had knowledge that almost no one else did, and that expertise in privacy was challenging to come by in the general population, and most particularly among the youngest members of society. There was broad agreement that communication to the youth about privacy risks and rights was a high priority area. A corollary theme was a general trend among the jurisdictions of 20 to 30 percent increases in the number of complaints regarding privacy. As awareness about privacy has grown, complaints have risen.

Regarding identity systems, some data protection authorities are specifically tasked with protecting identity data as part of their duties. Other DPAs have broad authority to protect sensitive and other types of data, which is inclusive of identity data. Most frequently mentioned were case studies regarding national registries; multiple Data Protection Authorities have worked to implement a national identity registry and have worked for better practices and management around collection, security, use, retention, and disclosure of identity data. Biometric data is among the data that multiple DPAs have worked to protect.

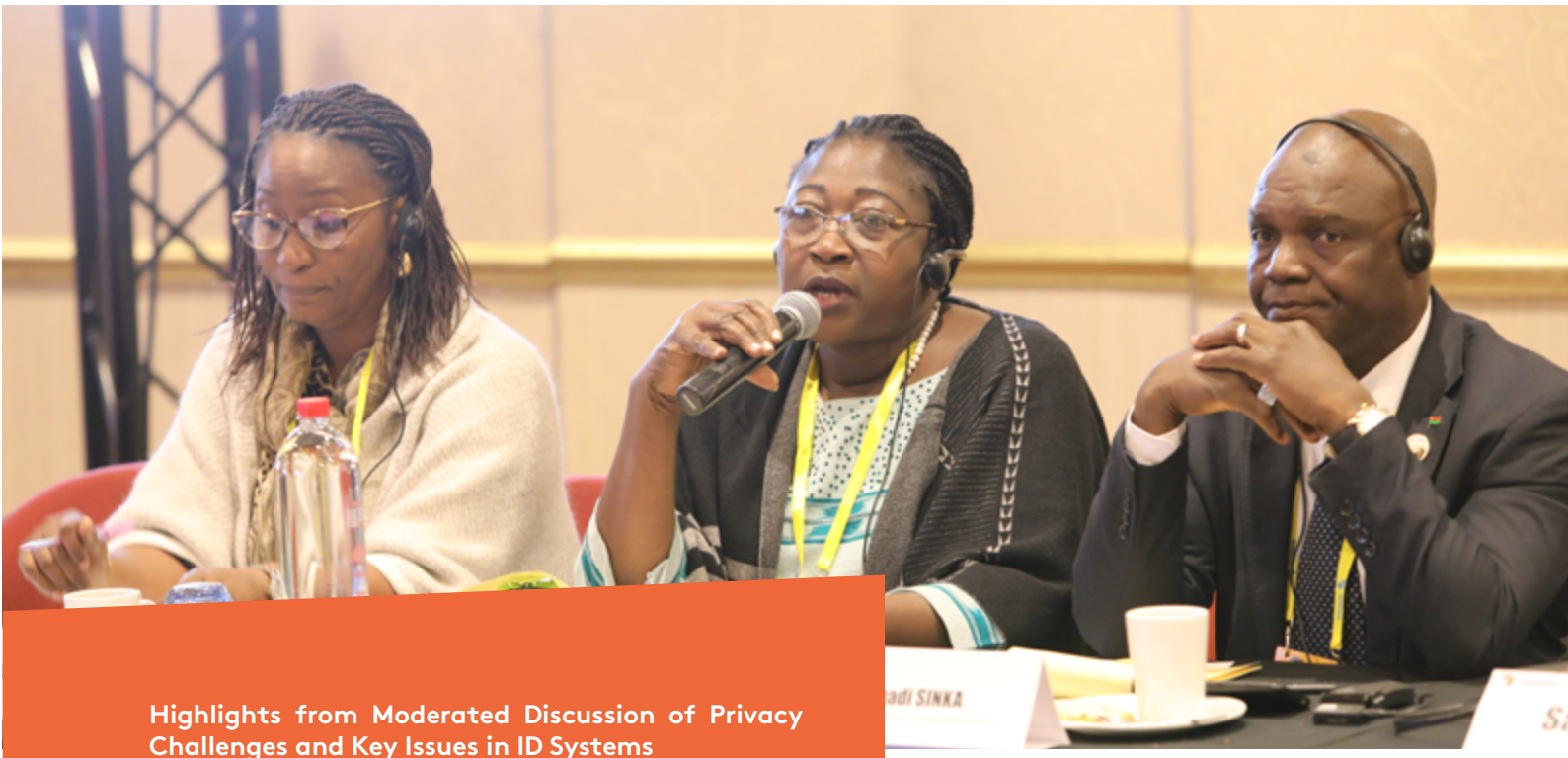
Enforcement of data protection laws was one of the recurring themes in the case studies. Biometric databases and other kinds of identity system databases (such as voter databases, and/or databases that include biometrics such as fingerprints or other biometrics) were mentioned as particularly sensitive. There was a discussion of data protection laws that ban the sale of certain types of databases containing sensitive identity information. There is variability in protections of this data, and there was concern that some jurisdictions in Africa have no protections against the sale of identity system data.

The presenters described a wide range of enforcement authority, and most noted that it was essential to work with multiple agencies and other parts of the government as cooperatively as possible. In the case of identity authorities, presenters noted that it was essential to form positive but independent collaborations in order to provide essential information and help to the authorities, who may be unfamiliar with data risks. Often, presenters needed to acquire new expertise in areas such as biometrics in efforts to fully understand data flows and assess privacy impacts.

A strong theme of country-level and international cooperation emerged from almost all of the presentations. There was much discussion of the need for common principles and a common vision for Africa, despite differences in population size, governmental structures, and other areas of differences. Experts repeatedly mentioned that Europe's General Data Protection Regulation, which came into force in May 2018, was having a pronounced impact on their need to harmonize country-level laws with the EU GDPR. Some of the countries have acceded to the Council of Europe Convention 108 on data protection (Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981). This is a treaty that is open for signature by member states and accession by non-member states. The DPAs noted that one of the drivers for international harmonization is also coming from businesses that were interested in being able to be compliant with the EU privacy standards.



III. DISCUSSION: CHALLENGES AND KEY ISSUES IN IDENTITY SYSTEMS AND PRIVACY



Highlights from Moderated Discussion of Privacy Challenges and Key Issues in ID Systems

- **The key challenge facing the Data Protection Authorities was the lack of consultation and cooperation by government officials regarding identity systems.**
- **Data Protection Authorities agreed that efforts to educate government officials and sensitize the public to data protection and privacy were central due to the lack of general privacy awareness in the population.**
- **DPAs noted a lack of resources regarding biometric and identity systems expertise and information, and expressed a desire to learn more about these systems.**
- **Many DPAs expressed that the lack of practical guidance to assist businesses and governments in implementing privacy laws was a key challenge. DPAs spoke about the difficulty of writing such guidance from scratch.**

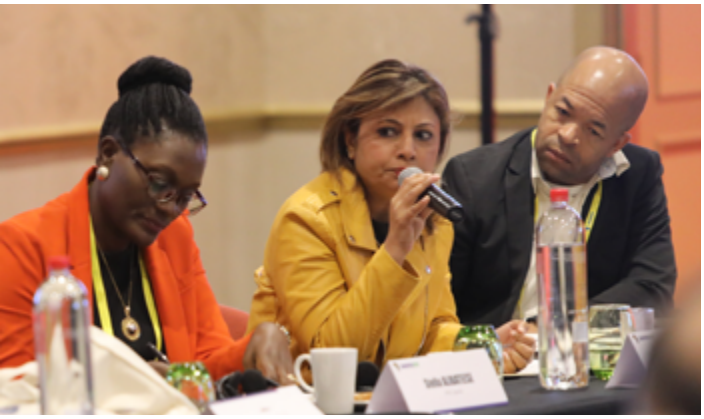
The moderated discussion segment of the workshop was focused on further exploration of the themes brought forward in the initial case studies, with a focus on key challenges and issues regarding privacy and identity systems. The participants had many experiences and challenges to share, and the conversation included a rich exchange of ideas and strategies. The conversation primarily focused on challenges in ID systems, with additional discussion about the role of practical guidance and the role of companies.

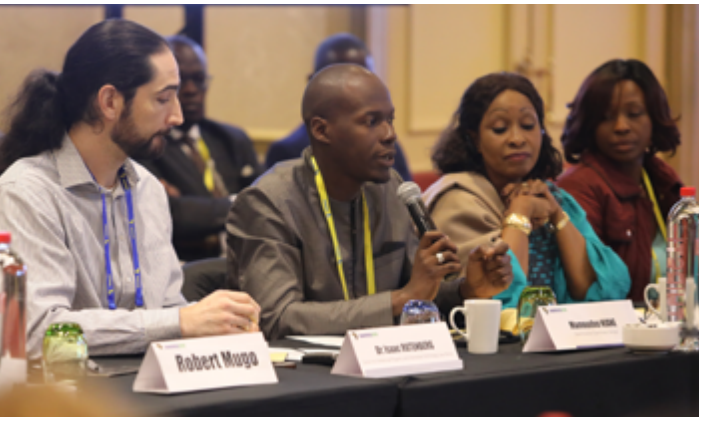
Overall, the moderated discussion around challenges in identity systems was the longest and most significant conversation of the roundtable meeting. Data protection authorities had multiple converging viewpoints of the specific challenges they faced at the country level.

Lack of Consultation and Cooperation

By far the most significant challenge brought forward by the roundtable participants was not being adequately consulted on identity system decisions, design, and implementation. This was an extremely common experience among the Data Protection Authorities, and it took many different forms, depending on the jurisdiction. However, even when laws were in place that required consultation, problems with lack of consultation existed. This portion of the roundtable discussions brought in opinions and ideas from almost every participant.

One participant discussed the lack of attention authorities in charge of identity systems give to Data Protection Authorities in general. Some serious lack of consultations had occurred in this DPA's jurisdiction; there were examples from election systems, where government authorities made decisions about these identity systems without any consent or consultation with Data Protection Authorities, even when it was required by law that they do so.





Another participant discussed their specific efforts to sensitize the administrators in charge of identity system management. Even though a data protection law was in place obligating the government to get consent from the DPA before implementing any decision, the government did not always comply. The DPA had to explain, advise, and push the government to consult with them regularly. Many DPAs expressed that they needed to consistently reach out to government agencies and identity authorities proactively in order to find a way to cooperate. This was not always successful, because "cooperation requires two willing parties," as one DPA put it.

Many DPAs expressed the need to sensitize and educate their governments and identity authorities about general data protection ideas, and explain why data protection is important. The DPAs noted that too often data protection is seen as something that is an obstacle, rather than an opportunity. Additionally, data protection is also viewed as a cost burden by governments and business. However, the general perspective the Data Protection Authorities voiced is that the loss of trust in the government or business due to poor handling of sensitive identity data is ultimately a far greater cost than what would have been paid to comply with data protection laws.

Some DPAs discussed the limits of voluntary cooperation, noting that enforcement actions are necessary when voluntary cooperation fails. Different countries provide for different levels of enforcement in this regard; some jurisdictions afford quite robust enforcement. Some of the DPAs had taken identity system enforcement actions in court, including legal actions around biometric databases and the handling and storage of biometric data.

One DPA had a specific case regarding an identity system, in this case, the DPA was able to successfully intervene regarding proposed changes to an electoral identity system that would have been deleterious. In this instance, the DPA had a good working relationship with the identity authority.

The DPAs agreed that voluntary cooperation and education was an extremely important tool in creating compliance in identity systems. But they also agreed that, particularly in identity systems, government administrators may be inclined to simply ignore data protection laws in the desire to get a system up and running. In those situations, enforcement actions may be necessary, if enforcement tools are available.

Lack of understanding about what data protection is (government, community)

A discussion around sensitizing governments and communities regarding the benefits of data protection revealed very similar challenges across jurisdictions. The DPAs discussed the overarching need to explain the basics of data protection and privacy, and continually persuade government administrators and members of the broader community of the benefits of data protection and privacy regulations. The DPAs broadly noted that privacy understanding was at a minimum in their jurisdictions, and a major mission of their office was to help reverse the lack of understanding around privacy.

One DPA contextualized the discussion of the need for data protection sensitization by noting that 10 to 15 years ago, security protections were similarly seen as burdensome. IT Security was seen as costly, and an obstacle — until it became clear that having weak security was more costly in the long run than paying for good security in the first place. The DPA compared the current privacy challenges to where the IT security arguments were 10 years ago.

Human Expertise in Identity Systems, including Biometrics

The DPAs discussed the need for informational resources and expertise regarding identity systems, noting that identity system experts were very difficult to find within their jurisdictions. Privacy expertise plus a knowledge of identity systems was a highly sought-after expertise, and rare.

One specific resource DPAs mentioned along these lines was a need for biometrics experts who were working in privacy, or who could consult regarding privacy. DPAs noted that they would appreciate and benefit from the availability of additional technical resources, information, and training around biometrics in particular due to the use of biometrics in identity systems.

Smart Cities Expertise

Smart cities and other emerging implementations of identity systems were another area where DPAs expressed the need for more informational resources and training. Several DPAs are being asked to evaluate smart city and other emerging types of complex systems where identity plays a central role. There are many technical components and issues to analyze in system in order to assess the privacy impacts, and DPAs would like to have more information at hand in order to make well-informed decisions.

There was a broad agreement that a variety of intelligent systems utilizing identity factors were emerging, and that preparation was important.

Role of Companies

Several DPAs and country level experts discussed the role of companies regarding identity and data protection. There was general agreement that multinational companies headquartered largely outside of the African Union had created a conundrum for the DPAs. On one hand, companies that are not from African countries want a lot of identity data from Africans. On the other hand, the DPAs did not have the ability to have a lot of control over how that data collection was occurring. One expert mentioned the troubling example of the sale of a large identity database from a particular African country to a commercial biometric company outside of the African Union, and how this is something that should not recur.

The DPAs expressed broad agreement that it would be positive to discuss data protection and privacy with companies, to understand expectations and to begin a dialogue around best practices and guidelines. One DPA expressed the issue by framing it as an issue of "sovereignty of the control of the data."

Role of Best Practices and Guidelines

The DPAs agreed that there was a lack of practical guidance available that implements country level data protection laws. The DPAs expressed a need across jurisdictions to create practical guidance that implemented country-level data protection laws. One DPA said, "We have laws, but not policies on data protection." DPAs discussed a need to harmonize practices in law enforcement and the use of identity information, and to create best practice guidance for this area.

Several DPAs mentioned projects to craft templates and create other automated tools to assist governments and business in implementing country level data protection laws. Some DPAs were in favor of facilitating self-regulation. All of the DPAs described having to invent and create practical implementations of their data protection laws. DPAs also were thinking about how to assist businesses in their countries in understanding and complying with EU's GDPR.

IV. FRAMEWORKS & HARMONIZATION

Highlights from Moderated Discussion of Privacy Frameworks

- **Data protection authorities largely agree that African countries want harmonized privacy principles; harmonized amongst African jurisdictions, and internationally.**
- **A key driver for harmonization is Europe's General Data Protection Regulation (GDPR), which is driving change in strengthening African data protection laws.**
- **Some African countries are seeking EU adequacy status, which is also heightening privacy protections in those jurisdictions.**
- **Stronger baseline privacy laws can create stronger baseline protections in identity systems.**

The topic of privacy frameworks and harmonization was a thread throughout the case studies and moderated discussion. There were several key aspects to the conversation. Most notably, Europe's General Data Protection Regulation (GDPR) has been extremely influential on data protection and privacy in Africa in a number of foundational ways.

First, there was broad agreement among the participants that Africa needed to have a unified vision of privacy, and unified principles around privacy, but developed by Africans and adapted to the needs of African countries. There was wide acknowledgement that the GDPR has set a new and higher baseline for privacy and data protection, and that privacy laws deemed weaker than GDPR would hamper growth and development over the long term. The participants had put a great deal of thought into the impact of GDPR on the continent of Africa, and the discussion was finely nuanced.

There was broad agreement that the most productive approach for harmonization would be to have unified principles consistent with the GDPR instead of attempting to unify larger and more detailed legislative frameworks with the GDPR. And a key point: participants wanted the unified principles to come from African DPAs and privacy experts to meet the needs of African countries.

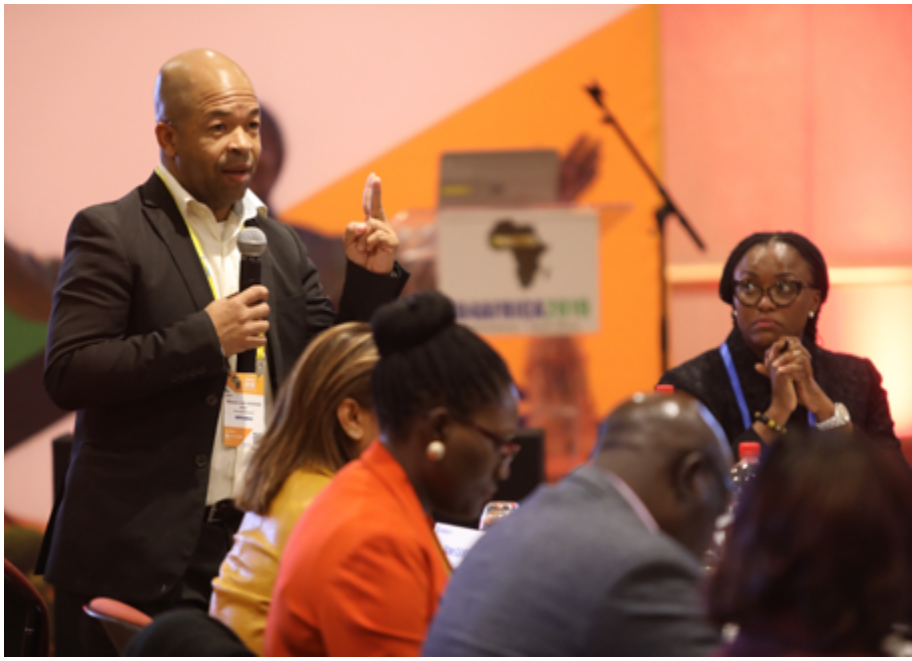
Second, in regards to privacy in identity systems, there was not a particular framework that participants put forward as a specific solution to protect identity systems, however, there was agreement that stronger overall data protection laws providing for independence and effective Data Protection Authorities with good enforcement tools would help provide greater protections for identity systems. One tool that data protection authorities agreed they could benefit from was increased cooperation regarding identity systems from authorities implementing identity registries and systems.

Third, participants noted the overlapping nature of data protection laws in Africa. There are country level data protection laws in many (but not all) African countries, regional data protection frameworks, federal data protection frameworks, and there is one international framework that was mentioned frequently.

The participants discussed comprehensive data protection legislation at the country level, as well as regional frameworks and federal and international agreements. Some of the participants noted that their legislatures had updated country-level laws to be stronger. Participants also discussed in passing regional frameworks in Africa, including ECOWAS, which is the Supplementary Act A/SA.1/01/10 on Personal Data Protection for the Economic Community of West African States. SADC is another framework operative on the African continent, it originates from the Data Protection Model Law 2012 for Southern African Development Community (SADC). In East African Community states, the EAC Legal Framework for Cyber Laws 2008 (Phase I) was adopted in 2010. These frameworks are still in place in multiple jurisdictions, however, they co-exist with the comprehensive country-level privacy and data protection regulations as well as federal agreements.

One particular federal framework, the African Union Convention on Cybersecurity and Personal Data Protection, which was adopted June 27, 2014, received a lot of discussion from the participants. The AU Convention covers electronic transactions, personal data protection, and cybercrime. The AU Convention, due to when it was originally written, is similar to the original EU Data Privacy Directive 95/46/EC, which has since been replaced by the GDPR. The original EU Data Privacy Directive has many similarities to the GDPR. The AU Convention remains an important influence and framework in Africa. The AU Convention is still open for signature, with the most recent signature dating from June 2019.

Participants had a robust discussion of the Council of Europe Convention 108 on data protection (Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981). The CoE Convention 108 is a treaty that is open for accession by African countries, and a number of participants were from jurisdictions that had acceded to the convention.



A fourth and final point to be made about the frameworks discussion is that at least one country has applied to receive an adequacy finding by the EU. This is a very significant step; in applying for adequacy, the Data Protection Authority has to ensure that the African country offers an adequate level of data protection that is comparable to the protections the GDPR supplies for Europeans. The impact of an adequacy decision is profound; such a decision would allow data to flow from the EU to the country with EU adequacy status without additional safeguards.

V. THE PATH FORWARD AND NEXT STEPS

Highlights from the Path Forward and Next Steps

- **Data protection authorities agreed that they would like to create guidance specific to identity systems.**
- **There was a unanimous desire to reconvene next year in order to continue work around how to improve privacy in identity systems.**
- **Data Protection Authorities would like to meet with identity authorities to have a closed door discussion regarding compliance.**
- **Data Protection Authorities would like to discuss best practices with industry and gather feedback.**

The discussion regarding the path forward and next steps centered on three key items: the creation of guidance for identity systems, a decision to reconvene next year, and specific requests for conversations in the next meeting.

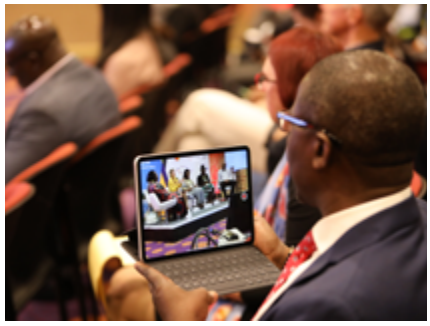
A first area the Data Protection Authorities found agreement on regarding a path forward was the decision to craft guidance specific to identity systems. There was a good amount of discussion regarding the logistics of this effort. A decision was made that the DPAs would hold a meeting to discuss the logistics amongst themselves and arrive at a decision about logistics after this consultation.

A second decision the DPAs came to was the unanimous decision to reconvene next year to further discussion and work on privacy in identity systems. The DPAs had several suggestions, with two in particular reaching consensus:

1. DPAs expressed a desire to have a closed-door meeting with identity authorities to hear them discuss how they are complying with country-level data protection laws.
2. DPAs also expressed a desire to meet with a group of industry representatives to discuss best practices and compare ideas and experiences.

There was a reiteration of themes expressed earlier in the meeting that ID4Africa could be of assistance particularly in providing expertise in the technical aspects of identity systems, whether that be by facilitating training, or via other educational materials.

VI. CONCLUSION



Africa is in the midst of a substantive transformation regarding data protection, privacy, and identity systems. Country-level comprehensive data protection regimes are being put in place in jurisdictions across the continent, with the last decade showing increases in adoption and awareness of privacy. For their part, the African Data Protection Authorities have an increasing body of experience implementing and enforcing their country-level data protection laws, as well as increasing connections and cooperation with each other and with international privacy peers.

This rich and increasing body of law, knowledge, and experience is beginning to yield results in identity systems as Data Protection Authorities seek to cooperate with and provide privacy and data protection guidance to identity authorities and others working with identity data.

While there are still many challenges ahead in regards to identity systems and privacy in African countries, progress has been made. The next five years will be crucial for strengthening existing data protection laws, and ensuring Data Protection Authorities have all of the tools and help they need as they seek to bring data protection and privacy to identity systems and data in African countries.

The Africa DPA discussions were rich and nuanced. Key observations from the RADPA discussions include the following points:

- African countries are rapidly developing and enacting comprehensive data protection and privacy laws. Also on the increase is the awareness and importance of international data protection laws, standards, and agreements.

- Data Protection Authorities have a great deal of experience with identity registries and systems, including those utilizing biometrics. DPAs have many ongoing concerns regarding the privacy risks of identity systems.

- One of the key challenges African DPAs face is the need to greatly increase meaningful and ongoing cooperation and communication with those parts of the government working with identity systems and systems containing identity data. Too often, identity authorities and other governmental offices are not aware of data protection laws or the need to cooperate with Data Protection Authorities. In some cases, government authorities implementing identity systems have ignored privacy regulations and Data Protection Authorities.

- There is a growing awareness of privacy and data protection among the public, and African Data Protection Authorities have seen privacy complaints rise 20-30 percent in the past few years.

- Going forward, a key task for African Data Protection Authorities will be to develop their own principles, harmonized between the African countries, and also harmonized to international privacy and data protection standards, particularly those articulated in the EU GDPR.

- Going forward, a key resource necessary for African Data Protection Authorities will be access to expertise and training regarding emerging identity systems technologies, including those used in new contexts such as smart cities.