6TH PRIVACY SYMPOSIUM AFRICA

Key Policy Recommendations

Theme:

Bridging Policy, Technology, and Societal Dynamics

19th – 21st Nov. 2024 | Harare, Zimbabwe

Published by: Unwanted Witness | 17th January, 2025

6TH PRIVACY SYMPOSIUM AFRICA

Key Policy Recommendations

INTRODUCTION

The th Privacy Symposium Africa (PSA), held from 19th to 21st November 2024 in Harare, Zimbabwe, convened a dynamic community of thought leaders, policymakers, technologists, and privacy advocates. Under the theme "Bridging Policy, Technology, and Societal Dynamics," the symposium provided a pivotal platform to explore the multifaceted dimensions of data protection and privacy in Africa. This annual gathering, organized by Unwanted Witness, has established itself as a cornerstone event in advancing privacy governance, addressing regional challenges, and proposing actionable solutions.

Overview of the 6th PSA and Its Objectives

Building on its mission since its inception in 2019, the 6th PSA embraced a sectoral lens approach, delving into the unique privacy and data governance challenges across critical sectors such as law, finance, health, telecommunications, and election data governance. This year's emphasis on Election Data Governance underscored the pressing need to safeguard transparency, integrity, and privacy within electoral processes, a cornerstone of democratic systems.

The event featured a rich program of masterclasses, panel discussions, and exclusive reports, all aimed at equipping stakeholders with the tools, insights, and networks needed to enhance privacy practices across the continent.
Masterclasses targeted specific audiences, such as lawyers, financial experts, and election officials, while the release of the Privacy Scorecard Report shed light on privacy practices in countries including Uganda, Kenya, Tanzania, Rwanda, Zimbabwe, and Mauritius, providing measurable benchmarks for progress.

Purpose of This Document

This document presents the key policy recommendations arising from the deliberations and insights shared during the symposium. It is intended for policymakers, data protection regulators, business leaders, academics, and civil society organizations who are vested in strengthening data governance across Africa. By consolidating expert opinions, real-world case studies, and actionable solutions, this paper aims to empower stakeholders with a roadmap for advancing data protection and privacy frameworks.

Acknowledgment

The success of the 6th PSA owes much to the distinguished speakers, moderators, and contributors who enriched the gathering with their expertise and perspectives. Esteemed panelists provided invaluable insights across diverse themes. Sessions were skillfully moderated by leaders, fostering engaging discussions that bridged gaps between policy, technology, and society.

Unwanted Witness extends profound gratitude to all participants for their contributions to this collective effort in shaping a privacy-respecting future for Africa. This document reflects their dedication and the shared commitment to building robust data protection ecosystems that prioritize human dignity, transparency, and trust.

Organized by: Unwanted Witness · Law Society of Zimbabwe · MISA Zimbabwe

In partnership with: Hewlett Foundation · Privacy International · Civil Rights Defenders · Open Society Foundations · accountabilitylab Zimbabwe

For more information: www.privacysymposiumafrica.com

6TH PRIVACY SYMPOSIUM AFRICA

OBJECTIVES OF THE RECOMMENDATIONS

a. Addressing pressing data protection and privacy issues in Africa.

b. Promoting effective collaboration among policymakers, regulators, private sector entities, and civil society.

c. Strengthening legal and regulatory frameworks.

OVERVIEW OF PANELS AT THE 6TH PRIVACY SYMPOSIUM AFRICA (PSA) 2024

The 6th Privacy Symposium Africa (PSA) focused on bridging policy, technology, and societal dynamics within the context of privacy and data protection in Africa. The panels were designed to foster discussions on pressing challenges, offer solutions, and highlight the evolving landscape of privacy across various sectors. Below is an overview of the key panels held during the symposium, each contributing to critical policy recommendations for strengthening privacy and data protection across the continent.

a. Proactive vs. Reactive Enforcement Strategies: Maximizing Impact in Data Protection Regulation (Conversation with Regulators)

This panel delved into the regulatory frameworks for data protection across African countries, emphasizing the importance of adopting proactive enforcement strategies. Experts highlighted the benefits of early intervention in ensuring compliance with data protection laws, as opposed to reactive measures that often arise post-violation.

Discussions centered on practical approaches to enhance regulatory capacity, reduce risks to privacy, and promote a culture of accountability.

The key policy recommendation stemming from this session advocates for strengthening the capacity of regulators to monitor and enforce privacy regulations proactively, ensuring that organizations comply with data protection laws before violations occur.

b. Strengthening Data Privacy and Protection in Zimbabwe: Examining the Gaps, Challenges, and Pathways to Accountability

Focused on Zimbabwe, this panel examined the current state of data protection in the country, identifying key gaps in legislation and enforcement. Stakeholders discussed the challenges faced by Zimbabwe in achieving full compliance with international privacy standards and ensuring the protection of citizens' personal data.

A major policy takeaway from this panel was the recommendation for a comprehensive review and strengthening of Zimbabwe's data privacy laws, along with enhanced accountability mechanisms for both public and private sector actors handling personal data.

c. Exploring Global Perspectives on AI Regulation in Data Protection and Extracting Lessons for Africa Amidst Weak Legal Frameworks

This session explored the intersection of artificial intelligence (AI) and data protection, analyzing global regulatory approaches to AI and data privacy. Experts discussed the implications of AI on personal privacy, especially within weak legal frameworks in many African countries. The panel emphasized the need for Africa to develop context-specific AI regulations that not only protect privacy but also foster innovation.

Policy recommendations highlighted the importance of establishing AI-specific data protection laws, focusing on transparency, accountability, and fairness, to safeguard citizens' privacy while encouraging technological growth.

Organized by: Unwanted Witness · Law Society of Zimbabwe · MISA Zimbabwe

In partnership with: Hewlett Foundation · Privacy International · Civil Rights Defenders · Open Society Foundations · accountabilitylab Zimbabwe

For more information: www.privacysymposiumafrica.com

d. Complexities of Election Data Management in Africa's Digital Democracy: Challenges and Opportunities

As a key thematic area, this panel addressed the challenges and opportunities of managing election-related data in Africa's evolving digital democracy. The session examined the risks of data breaches, manipulation, and misuse in electoral processes, while also exploring opportunities for improving electoral integrity through better data governance practices. The session underscored the importance of establishing robust election data management frameworks and recommended enhancing transparency in the collection, processing, and storage of electoral data to safeguard voter privacy and ensure the integrity of the democratic process.

e. Data Breach Preparedness and Response: Mitigating Risks and Restoring Trust in Financial Institutions

This panel focused on the financial sector's approach to data breach preparedness and response. With the increasing incidence of cyberattacks and data breaches, the discussion revolved around the need for robust incident response plans and mitigation strategies to protect financial data and restore public trust.

Key policy recommendations included the development of stringent data protection protocols for financial institutions and the establishment of industry-specific standards for responding to breaches, along with public notification practices that prioritize transparency and accountability.

f. Harnessing the Power of AI – What Does It Mean to the Concept of Humanity?

A philosophical and ethical exploration, this panel discussed the implications of AI on human dignity and privacy. Experts debated the potential risks of AI-driven surveillance, profiling, and decision-making on individuals' fundamental rights. The session brought forward policy recommendations advocating for the incorporation of human rights principles into AI design and regulation, ensuring that AI technologies are developed and deployed in ways that respect and uphold human dignity.

g. Privacy Mishaps: Funny and Sad Stories from the Workplace

This lighter, yet informative session shared real-life stories of privacy breaches and mishaps in the workplace, highlighting the human side of data protection challenges. Through humorous and somber anecdotes, the panel emphasized the importance of cultivating a privacy-conscious culture within organizations.

The key takeaway for policymakers was the need for comprehensive privacy training programs and clear organizational policies to reduce accidental breaches and enhance employees' understanding of privacy responsibilities.

h. Privacy in the Age of Social Media: Are We All Oversharing?

In the age of social media, this panel tackled the issue of oversharing personal data and its implications for privacy.

Experts discussed how individuals' personal data is

increasingly exposed on social platforms and the risks it poses to privacy. Discussions revolved around educating the public on managing their digital footprint and holding platforms accountable for protecting user data. A major policy recommendation emphasized the need for stronger regulations governing social media platforms, with a focus on user consent, data retention policies, and ensuring transparency in data usage.

i. Surveillance, Privacy, and the Future of Democracy in Africa

This session explored the balance between state surveillance and individual privacy in Africa, particularly in the context of growing concerns over surveillance technologies and their impact on democratic freedoms. Panelists discussed the potential dangers of unchecked surveillance and its consequences for political rights, freedom of expression, and privacy.

The policy recommendation emerging from this discussion called for the introduction of legal safeguards to regulate state surveillance practices and ensure that they do not infringe upon citizens' privacy and civil liberties.

j. Let's Talk: Data Protection and Elections in Africa

A candid conversation that explored the critical role of data protection in elections across Africa. It focused on how to safeguard electoral data, address challenges in voter data management, and promote transparency during elections.

Key policy recommendations included strengthening data protection measures within election processes and ensuring the independence of election commissions to enhance the integrity of electoral data management.

PANEL-SPECIFIC POLICY RECOMMENDATIONS

i. Title: *Strengthening Data Privacy and Protection in Zimbabwe: Examining the Gaps, Challenges, and Pathways to Accountability*

Brief description of the topic and context

In the digital era, safeguarding personal data has become critical to protecting individuals' privacy, rights, and freedoms. Zimbabwe's Data Protection Act (DPA) of 2021 establishes a framework for data privacy and protection. However, stakeholders have identified key gaps, including the lack of breach notification provisions, the absence of guaranteed independence for the data protection authority (DPA), and limited pathways for data subjects to seek remedies for violations. These gaps hinder accountability and weaken trust in the system.

This panel at the 6th Privacy Symposium Africa explored these issues, examined Zimbabwe's current legislative and regulatory framework, and proposed pathways to strengthen data protection and accountability.

Key Policy Recommendations

Recommendation 1: Introduce Mandatory Data Breach Notification Provisions

Action Needed:

Amend the Cyber and Data Protection Act (CDPA) of Zimbabwe to include a mandatory provision requiring data controllers and processors to notify affected data subjects and the data protection authority of any data breaches within a specified timeframe. The provision should also require public disclosure of major breaches to enhance transparency.

6TH PRIVACY SYMPOSIUM AFRICA

Responsible Party:
Parliament of Zimbabwe, Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), and relevant ministries.

Impact:
This will enhance transparency, allow data subjects to take precautionary measures, and promote accountability among data controllers and processors. It will also build public trust in data protection systems.

Recommendation 2: Guarantee the Independence of the Data Protection Authority

Action Needed:
Amend the governance structure of the Data Protection Authority to ensure its operational and financial independence. Establish separate oversight mechanisms for the Cybersecurity Centre to prevent conflicts of interest and overreach by the Office of the President.

Responsible Party:
Parliament of Zimbabwe, the Ministry of Information Communication Technology, Postal and Courier Services, and civil society organizations (CSOs) advocating for independent oversight.

Impact:
An independent DPA will ensure impartial enforcement of data protection laws, reduce the potential for political influence, and foster greater accountability.

Recommendation 3: Empower the DPA with Sanctioning Authority

Action Needed:
Amend the Cyber and Data Protection Act (CDPA) of Zimbabwe to grant the DPA powers to impose administrative sanctions, fines, and other penalties on entities that violate data protection laws.

Responsible Party:
POTRAZ, Parliament of Zimbabwe, and the Ministry of Justice, Legal and Parliamentary Affairs.

Impact:
Sanctioning authority will strengthen enforcement, deter non-compliance, and encourage proactive measures among data controllers and processors to protect personal data.

Recommendation 4: Establish a Right to Compensation for Data Subjects

Action Needed:
Amend the Cyber and Data Protection Act (CDPA) of Zimbabwe to provide explicit provisions allowing data subjects to seek compensation through the courts for damages resulting from breaches of the law. Create streamlined processes for reporting and addressing grievances.

Responsible Party:
Parliament of Zimbabwe, the Judiciary, and civil society organizations advocating for human rights and consumer protection.

Impact:
This will empower individuals to assert their rights, deter violations, and create a culture of accountability in data protection.

6TH PRIVACY SYMPOSIUM AFRICA

Recommendation 5: Foster Multi-Stakeholder Engagement on Data Protection

Action Needed:
Establish a permanent, multi-stakeholder advisory group comprising government entities, private sector actors, civil society organizations, and academia to provide input on the implementation, monitoring, and continuous improvement of data protection policies.

Responsible Party:
POTRAZ, civil society organizations, private sector stakeholders, and academic institutions.

Impact:
Multi-stakeholder collaboration will ensure inclusive policymaking, address emerging data protection challenges, and improve the overall governance framework.

Recommendation 6: Build Awareness and Capacity on Data Protection

Action Needed:
Launch public awareness campaigns on the rights and responsibilities under the Cyber and Data Protection Act (CDPA) of Zimbabwe and provide capacity-building initiatives for stakeholders, including data controllers, processors, and law enforcement agencies.

Responsible Party:
POTRAZ, Ministry of Education, civil society organizations, and private sector actors.

Impact:
Increased awareness will empower individuals to exercise their rights and ensure that data controllers and processors comply with legal and ethical standards.

Recommendation 7: Align Data Protection Policies with Global Best Practices

Action Needed:
Conduct a comparative review of international data protection frameworks (e.g., GDPR) and incorporate relevant best practices into Zimbabwe's legislation.

Responsible Party:
POTRAZ, Ministry of ICT, and international experts in data protection.

Impact:
Harmonizing Zimbabwe's data protection policies with global standards will improve its international standing, attract investment, and ensure the protection of citizens' data in cross-border contexts.

6TH PRIVACY SYMPOSIUM AFRICA

ii. Title: *Proactive vs. Reactive Enforcement Strategies: Maximizing Impact in Data Protection Regulation (Conversation with Regulators)*

Brief Description of the Topic and Context

This panel discussion explored the effectiveness of proactive versus reactive enforcement strategies in the realm of data protection regulation.
As technological advancements continue to redefine how data is collected, stored, and utilized, regulators face the dual challenge of preventing data breaches while effectively responding tincidents when they occur. The discussion assessed the strengths, weaknesses, and implementation challenges of both strategies, while providing actionable insights into optimizing enforcement efforts to better safeguard privacy rights.
The conversation underscored the need for a balanced approach, integrating proactive and reactive enforcement strategies to enhance compliance, build trust, and protect citizens' data in an increasingly digital world.

Key Policy Recommendations

Recommendation 1: Institutionalize Predictive Data Analytics for Proactive Enforcement

Action Needed:
Regulatory bodies should invest in advanced data analytics and machine learning tools to identify and mitigate potential data protection risks before breaches occur.

Responsible Party:
National Data Protection Authorities (DPAs), government ministries overseeing technology and innovation, private technology firms, and international data protection alliances.

Impact:
This approach will enhance early detection of vulnerabilities, reduce the frequency and impact of data breaches, and position regulators as leaders in modern enforcement practices.

Recommendation 2: Foster Public-Private Collaboration for Data Security Innovation

Action Needed:
Develop frameworks for collaboration between regulators and private organizations to co-create and pilot proactive compliance tools, such as privacy-by-design protocols and automated compliance check systems.

Responsible Party:
DPAs, private technology companies, industry associations, and academic institutions.

Impact:
Collaborative innovation will drive adoption of best practices, enhance industry compliance, and encourage shared accountability for protecting personal data.

Recommendation 3: Implement Tiered Guidance and Educational Programs for Organizations

Action Needed:
Develop sector-specific guidelines and training programs to educate organizations on compliance expectations, focusing on proactive measures such as data privacy audits and secure data handling protocols.

6TH PRIVACY SYMPOSIUM AFRICA

Responsible Party:
DPAs, industry regulators, and professional training organizations.

Impact:
Proactive education will reduce the likelihood of unintentional non-compliance, empower organizations to adopt preventative measures, and improve overall compliance rates.

Recommendation 4: Introduce Dual-Mode Enforcement Frameworks

Action Needed:
Adopt regulatory frameworks that blend proactive and reactive measures, such as combining guidance and audits with penalties for non-compliance or breaches.

Responsible Party:
National DPAs, legal advisory bodies, and legislative committees.

Impact:
This balanced approach ensures organizations are both supported in implementing preventative strategies and held accountable when breaches occur, fostering trust and compliance.

Recommendation 5: Establish Cross-Border Data Protection Knowledge Sharing

Action Needed:
Facilitate knowledge exchange between jurisdictions, particularly leveraging successful proactive enforcement models like those implemented in Estonia and other European nations.

Responsible Party:
African Union, international data protection organizations, and intergovernmental bodies.

Impact:
Cross-border knowledge sharing will accelerate the adoption of proven strategies, improve regulatory effectiveness, and support harmonization of data protection standards across Africa.

Recommendation 6: Strengthen Emergency Response Units for Reactive Enforcement

Action Needed:
Establish specialized units within DPAs dedicated to swift incident response, equipped with resources to investigate breaches and enforce penalties in real-time.

Responsible Party:
National DPAs, cybersecurity authorities, and public safety departments.

Impact:
Enhancing reactive capacity will enable rapid responses to breaches, mitigate damage to individuals, and deter future violations through timely enforcement.

Recommendation 7: Integrate Data Protection Regulation into National Development Agendas

Action Needed:
Position data protection as a key pillar in national digital transformation strategies, ensuring sustained funding, capacity-building, and alignment with broader development goals.

Responsible Party:
National governments, DPAs, and international development partners.

Organized by: Unwanted Witness · Law Society of Zimbabwe · MISA Zimbabwe

In partnership with: Hewlett Foundation · Privacy International · Civil Rights Defenders · Open Society Foundations · accountabilitylab Zimbabwe

For more information: www.privacysymposiumafrica.com

Impact:
This will ensure data protection remains a national priority, while fostering innovation and economic growth in digital services.

iii. Title: *Exploring Global Perspectives on AI Regulation in Data Protection and Extracting Lessons for Africa Amidst Weak Legal Frameworks*

Brief Description of the Topic and Context

This panel explored the complexities of Artificial Intelligence (AI) regulation in the context of data protection, focusing on lessons from global frameworks that Africa can adopt. The discussion highlighted the challenges posed by Africa's nascent legal and regulatory structures amidst rapid technological advancements. Panelists and participants emphasized the need for AI governance frameworks that safeguard data privacy while addressing ethical and societal concerns unique to the African context.

Key Policy Recommendations

Recommendation 1: Establish Comprehensive AI Governance Frameworks

Action Needed:
African countries should establish and adopt AI governance frameworks that balance innovation with robust safeguards for data privacy and human rights. These frameworks must incorporate ethical principles, risk assessment mechanisms, and provisions for algorithmic transparency and accountability.

Responsible Party:
National governments, regional bodies like the African Union, and regulatory agencies.

Impact:
Provides clear guidelines for AI development, minimizes misuse of AI technologies, and fosters public trust while aligning with global standards.

Recommendation 2: Strengthen Regional and Cross-Border Collaboration

Action Needed:
Develop regional AI regulatory strategies through collaboration among African countries. Establish standardized policies and data-sharing agreements to ensure consistent application of AI governance principles across borders.

Responsible Party:
African Union, East African Community (EAC), Southern African Development Community (SADC), and regional data protection authorities.

6TH PRIVACY SYMPOSIUM AFRICA

Impact:
Promotes regional harmonization, addresses cross-border data issues, and creates a unified voice in global AI policy discussions.

Recommendation 3: Empower Civil Society and Grassroots Organizations

Action Needed:
Engage civil society organizations and grassroots initiatives in shaping AI regulation and data protection policies. Support these organizations through funding, training, and inclusion in policymaking processes.

Responsible Party:
Governments, international development partners, and civil society organizations.

Impact:
Amplifies marginalized voices, ensures policies are people-centered, and promotes transparency and accountability in governance.

Recommendation 4: Build Capacity for Legal and Technical Expertise

Action Needed:
Invest in training programs for legal professionals, policymakers, and technical experts on AI governance, with a focus on ethical AI, legal tech solutions, and data privacy frameworks.

Responsible Party:
Academic institutions, professional organizations, and governments.

Impact:
Enhances the capacity of stakeholders to develop and implement effective regulations while addressing local challenges.

Recommendation 5: Foster Innovation-Friendly Regulatory Environments

Action Needed:
Design AI regulatory frameworks that incentivize innovation while ensuring compliance with data protection laws. This includes establishing sandboxes for testing AI technologies in a controlled environment.

Responsible Party:
Governments, private sector innovators, and international organizations.

Impact:
Encourages growth in AI innovation and investment in Africa, while maintaining safeguards for data privacy and security.

Recommendation 6: Prioritize Digital Literacy and Public Awareness

Action Needed:
Develop and implement digital literacy programs that educate the public on AI technologies, data privacy, and their rights in digital environments.

Responsible Party:
Governments, educational institutions, and non-governmental organizations.

Impact:
Empowers individuals to make informed decisions about their data and enhances societal resilience to AI-related challenges.

Recommendation 7: Align AI Governance with Human Rights Protections

Action Needed:
Embed human rights principles into AI policies and ensure mechanisms for monitoring and addressing violations, especially in regions with weak legal frameworks.

Responsible Party:
Governments, human rights organizations, and regional legal bodies.

Impact:
Protects individuals from harm caused by AI technologies and ensures alignment with international human rights standards.

Recommendation 8: Establish Public-Private Partnerships for AI Governance

Action Needed:
Encourage collaboration between governments and private sector stakeholders to co-develop ethical AI standards, share best practices, and invest in regulatory infrastructure.

Responsible Party:
Governments, tech companies, and industry associations.

Impact:
Enhances the implementation of AI governance policies and accelerates technological advancements in a responsible manner.

iv. Title: *Complexities of Election Data Management in Africa's Digital Democracy: Challenges and Opportunities*

Description of the Topic and Context

The panel explored the transformative impact of digital technologies on election data management in Africa.

As electronic voting systems, digital voter registries, and AI-driven analytics become integral to electoral processes, they bring both opportunities and challenges. These include enhancing transparency and efficiency while raising concerns about data privacy, cybersecurity, inclusivity, and the integrity of democratic processes.
The panel featured insights from diverse experts and emphasized the need for innovative, collaborative, and robust solutions to address these pressing issues.

Key Policy Recommendations

Recommendation 1: Strengthening Election Data Governance Frameworks

Action Needed:
Develop and implement comprehensive election data governance frameworks that clearly define data collection, storage, processing, sharing, and disposal protocols. These frameworks should include strict provisions for consent, purpose limitation, and accountability.

Responsible Party:
Election Management Bodies (EMBs), National Data Protection Authorities, Regional organizations like the African Union (AU)

6TH PRIVACY SYMPOSIUM AFRICA

Impact:
Establishing robust governance frameworks ensures that personal data collected during electoral processes is used responsibly, minimizing risks of misuse, political profiling, and voter manipulation. It enhances public trust in digital election systems and protects the integrity of democratic processes.

Recommendation 2: Leveraging EmergingTechnologies for Transparency and Security

Action Needed:
Promote the adoption of emerging technologies, such as blockchain and AI, to enhance transparency and security in election data management. Blockchain can ensure immutable voter registries, while AI can preemptively detect and mitigate misinformation campaigns.

Responsible Party:
Election Management Bodies, National ICT Ministries, Technology providers

Impact:
These technologies increase the reliability and security of election data, reduce risks of tampering and fraud, and empower citizens to trust and actively participate in democratic processes.

Recommendation 3: Enhancing Cybersecurity Measures for Election Systems

Action Needed:
Mandate regular cybersecurity audits, establish national election cybersecurity task forces, and develop contingency plans to respond to cyber threats targeting election data infrastructure.

Responsible Party:
Election Management Bodies, National Cybersecurity Agencies, Private sector, cybersecurity firms.

Impact:
Improved cybersecurity safeguards election systems against hacking, data breaches, and other cyber threats, preserving the confidentiality and accuracy of election data.

Recommendation 4: Promoting Inclusivity and Accessibility

Action Needed:
Design and implement election data systems that are inclusive of marginalized and vulnerable populations, ensuring accessibility in remote areas and for individuals with disabilities.

Responsible Party:
Election Management Bodies, Civil society organizations, International development partners.

Impact:
Inclusive systems reduce disenfranchisement, ensuring that all citizens, regardless of socioeconomic or geographic status, can participate in electoral processes. This reinforces democratic values and representation.

Recommendation 5: Establishing Collaborative Oversight Mechanisms

Action Needed:
Create multi-stakeholder oversight committees, including civil society, data protection authorities, and election observers, to monitor compliance with data protection standards and investigate complaints of data misuse during elections.

Organized by: UNWANTED WITNESS · Law Society of Zimbabwe · MISA ZIMBABWE

In partnership with: Hewlett Foundation · PRIVACY INTERNATIONAL · CIVIL RIGHTS DEFENDERS · OPEN SOCIETY FOUNDATIONS · accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

6TH PRIVACY SYMPOSIUM AFRICA

Responsible Party:
Election Management Bodies, Civil Society Organizations, International election monitoring bodies

Impact:
Collaborative oversight builds accountability and ensures that election data management aligns with best practices, deterring potential abuses and reinforcing public trust.

Recommendation 6: Building Capacity through Training and Awareness

Action Needed:
Provide regular training for EMB staff, political parties, and civil society organizations on data privacy, cybersecurity, and the ethical use of election data.
Conduct public awareness campaigns to educate citizens on their data rights during elections.

Responsible Party:
Election Management Bodies, National Data Protection Authorities, International development organizations.

Impact:
Increased capacity and awareness foster a culture of responsibility and ethical practices in election data management, empowering stakeholders and citizens to advocate for transparent and secure electoral processes.

Recommendation 7: Adopting International Standards and Best Practices

Action Needed:
Adopt and localize international data protection standards, such as the GDPR, to guide the management of sensitive election data in African contexts. Develop regional guidelines through the African Union to ensure uniformity and cooperation across member states.

Responsible Party:
National Data Protection Authorities, African Union (AU), Election Management Bodies

Impact:
Harmonizing data protection standards ensures a consistent approach to managing election data, fosters regional collaboration, and strengthens Africa's position in the global data governance discourse.

Recommendation 8: Mitigating Misinformation and Disinformation

Action Needed:
Establish real-time monitoring systems to detect and combat misinformation campaigns during election periods.
Empower civil society and media organizations with tools and resources to debunk false narratives effectively.

Responsible Party:
Election Management Bodies, Media regulators and organizations, Civil society organizations.

Impact:
Combating misinformation protects the credibility of electoral processes, prevents voter manipulation, and enhances informed civic participation.

Organized by: Unwanted Witness · Law Society of Zimbabwe · MISA Zimbabwe

In partnership with: Hewlett Foundation · Privacy International · Civil Rights Defenders · Open Society Foundations · accountabilitylab Zimbabwe

For more information: www.privacysymposiumafrica.com

6TH PRIVACY SYMPOSIUM AFRICA

v. Title: *Data Breach Preparedness and Response: Mitigating Risks and Restoring Trust in Financial Institutions*

Introduction and Context

The financial services sector is increasingly vulnerable to data breaches as cyberattacks grow in sophistication and frequency. With sensitive customer data at stake, breaches not only result in financial losses but also damage consumer trust, corporate reputation, and compliance status. This panel discussion at the 6th Privacy Symposium Africa (PSA2024) explored the current vulnerabilities in financial institutions and identified strategies to strengthen data breach preparedness and response frameworks.
It also emphasized the importance of cross-sector collaboration and innovative regulatory approaches to build resilience in the face of emerging threats.

Key Policy Recommendations

Recommendation 1: Strengthen Cybersecurity Preparedness through Proactive Measures

Action Needed:
Mandate financial institutions to develop comprehensive, institution-specific incident response plans, conduct regular penetration testing, and maintain continuous threat monitoring using AI-powered tools.

Responsible Party:
Financial institutions (banks, payment processors, etc.), regulators, and cybersecurity solution providers.

Impact:
Early identification and mitigation of threats, reduced downtime during breaches, and enhanced customer trust through demonstrated commitment to data security.

Recommendation 2: Enhance Data Breach Reporting and Regulatory Compliance Mechanisms

Action Needed:
Introduce clear, enforceable guidelines for mandatory breach reporting within 72 hours of detection. Regulators should provide training programs for compliance officers in financial institutions.

Responsible Party:
Data protection regulators (e.g., Data Protection Authorities), financial sector regulators, and compliance teams within financial institutions.

Impact:
Improved regulatory oversight, faster response to breaches, and better alignment with global standards like the GDPR, ensuring reduced penalties and reputational damage.

Recommendation 3: Foster Cross-Sector Collaboration for Threat Intelligence Sharing

Action Needed:
Establish national and regional platforms for financial institutions to share anonymized threat intelligence and best practices in breach prevention and response.

Responsible Party:
Governments, central banks, data protection authorities, and industry associations.

Impact:
Enhanced collective cybersecurity resilience across the sector, rapid response to emerging threats, and prevention of repeated attacks exploiting the same vulnerabilities.

6TH PRIVACY SYMPOSIUM AFRICA

Recommendation 4: Build Consumer Awareness and Transparency Protocols

Action Needed:
Require financial institutions to develop consumer education campaigns to raise awareness about phishing, fraud, and other cyber threats. Institutions must also establish clear communication protocols to notify consumers about breaches and remediation steps.

Responsible Party:
Financial institutions, marketing/PR teams, and consumer advocacy groups.

Impact:
Increased consumer vigilance, reduced success rates of social engineering attacks, and restoration of consumer trust after breaches.

Recommendation 5: Prioritize Legal and Corporate Governance Integration in Cybersecurity

Action Needed:
Implement board-level oversight for cybersecurity through mandatory inclusion of data security experts. Develop corporate governance frameworks that integrate data protection and breach response as core responsibilities.

Responsible Party:
Financial institution leadership (boards and executives), corporate governance advisors, and legal consultants.

Impact:
Strengthened institutional accountability, improved alignment of cybersecurity goals with corporate strategies, and a culture of proactive risk management.

Recommendation 6: Leverage Technology for Advanced Breach Prevention

Action Needed:
Invest in advanced cybersecurity tools such as AI/ML for threat detection, blockchain for secure transactions, and biometric authentication to minimize breach risks.

Responsible Party:
Financial institutions and technology providers.

Impact:
Enhanced fraud detection, reduced attack surfaces, and improved customer experience through the adoption of cutting-edge security measures.

Recommendation 7: Develop Tailored Regulatory Frameworks for Emerging Markets

Action Needed:
Design flexible data protection regulations for African financial institutions that consider unique regional challenges, such as cross-border transactions and technology gaps.

Responsible Party:
National governments, regional economic bodies, and global organizations such as the African Union (AU).

Impact:
Encourages innovation while maintaining robust data protection standards, ensuring compliance without stifling growth in emerging markets.

vi. Title: *Harnessing the Power of AI – What Does It Mean to the Concept of Humanity*

Brief Description of the Topic and Context

This panel explored the transformative potential of artificial intelligence (AI) while emphasizing the ethical, regulatory, and societal considerations required to ensure its alignment with human dignity and fundamental rights. Discussions centered on the regulatory landscape, balancing innovation with control, and the global challenges of managing AI in a localized context.

Additionally, the panel highlighted the role of AI in journalism, freedom of expression, and transparency in AI systems as critical areas requiring urgent attention.

Key Policy Recommendations

Recommendation 1: Strengthen AI-Specific Data Privacy Regulations

Action Needed:

Develop comprehensive regulations addressing data privacy concerns in AI, including the collection, processing, and use of personal data in AI-driven systems. Ensure AI algorithms meet privacy standards by incorporating measures like privacy-by-design and differential privacy.

Responsible Party:

National governments, data protection authorities, and AI developers.

Impact:

These measures will foster public trust in AI systems by safeguarding individual privacy, reducing misuse of personal data, and enabling responsible innovation.

Recommendation 2: Mandate Algorithmic Transparency and Accountability

Action Needed:

Require AI developers and companies to disclose information about their algorithms, including how they function, their decision-making processes, and measures taken to avoid bias. Establish independent oversight
bodies to evaluate and audit AI systems.

Responsible Party:

International standards organizations, national regulators, and AI industry leaders.

Impact:

Transparency will help prevent biases, ensure accountability, and empower users to understand and challenge AI-driven decisions.

Recommendation 3: Upskilling and Workforce Development for AI Ecosystems

Action Needed:

Implement national programs to upskill citizens in AI-related fields, including semiconductor manufacturing and AI ethics, to reduce dependence on imported technologies and infrastructure.

Responsible Party:

Ministries of education and technology, universities, and private sector stakeholders.

6TH PRIVACY SYMPOSIUM AFRICA

Impact:
Empowering local populations with AI-related skills will stimulate economic growth, create jobs, and reduce the costs of adopting AI technologies.

Recommendation 4: Foster Regional and Global Regulatory Harmonization

Action Needed:
Promote international collaboration to establish consistent AI regulatory standards while accounting for regional and local contexts. Convene regional dialogues to identify shared priorities and challenges, ensuring inclusivity for Global South nations.

Responsible Party:
Regional economic blocs (e.g., AU), global institutions (e.g., OECD, UN), and national governments.

Impact:
Harmonized standards will enhance cross-border cooperation, prevent regulatory fragmentation, and ensure equitable development of AI technologies globally.

Recommendation 5: Encourage AI for Public Good in Journalism and Media

Action Needed:
Invest in AI applications for journalism, including fact-checking tools, media literacy campaigns, and AI-driven systems promoting diverse perspectives. Establish ethical guidelines for AI use in content generation and moderation.

Responsible Party:
Media organizations, technology developers, and civil society groups.

Impact:
Strengthened public trust in media through improved accuracy and representation, reducing the spread of misinformation and harmful content.

Recommendation 6: Ensure Freedom of Expression in AI Systems

Action Needed:
Develop regulations to monitor and mitigate the misuse of AI algorithms for content censorship, manipulation of public opinion, or restriction of access to information. Implement mechanisms for human oversight in AI content moderation systems.

Responsible Party:
Digital rights advocacy groups, technology developers, and government regulators.

Impact:
Protecting freedom of expression while addressing harmful content will ensure democratic principles are upheld in the digital age.

Recommendation 7: Mandate Transparency and Explainability in AI Systems

Action Needed:
Introduce legal requirements for AI systems to clearly communicate their purposes, functionalities, and limitations to users. AI-driven decisions, especially in critical areas like finance and healthcare, should be explainable to users.

Responsible Party:
Policymakers, AI developers, and international standards bodies.

Organized by: UNWANTED WITNESS · Law Society of Zimbabwe · MISA ZIMBABWE

In partnership with: Hewlett Foundation · PRIVACY INTERNATIONAL · CIVIL RIGHTS DEFENDERS · OPEN SOCIETY FOUNDATIONS · accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

Impact:
Enhanced transparency will build trust, reduce societal resistance to AI adoption, and allow for greater public accountability.

Recommendation 8: Support AI Literacy for Empowered Users

Action Needed:
Launch public awareness campaigns and educational initiatives to improve AI literacy among citizens. Equip individuals with skills to critically evaluate AI-generated content and detect potential biases.

Responsible Party:
Educational institutions, civil society organizations, and government agencies.

Impact:
Empowered and informed citizens will contribute to a more resilient society capable of effectively navigating the challenges of AI systems.

vii. Title: *Surveillance, Privacy, and the Future of Democracy in Africa*

Brief Description of the Topic and Context

This panel examined the growing use of surveillance technologies by governments in Africa and their impact on democracy. While surveillance is often justified as a tool to enhance national security, it increasingly encroaches on individual privacy and civil liberties, especially in fragile democracies.
The session explored the tension between state surveillance and democratic governance, focusing on legal, ethical, and societal implications, and identifying actionable steps to balance security with privacy.

Key Policy Recommendations

Recommendation 1: Establish Comprehensive Data Privacy and Surveillance Laws

Action Needed:
Develop and implement clear, robust legal frameworks that govern the use of surveillance technologies in Africa. These laws must include:

- Mandatory transparency and accountability requirements for state and private surveillance actors.
- Provisions for judicial oversight of surveillance activities.
- Clear limits on data collection, storage, and use.

Responsible Party:
National governments and parliaments, Regional bodies such as the African Union (AU), Legal practitioners and civil society organizations.

6TH PRIVACY SYMPOSIUM AFRICA

Impact:

- Strengthens citizen trust in democratic governance by ensuring privacy rights are protected.
- Reduces the misuse of surveillance technologies against marginalized groups and political opponents.
- Aligns national laws with international privacy and human rights standards.

Recommendation 2: Foster Independent Oversight Bodies for Surveillance Activities

Action Needed:

Establish independent institutions to oversee government and private surveillance practices. These bodies must:

- Conduct regular audits of surveillance programs
- Investigate complaints of abuse and ensure
- accountability.
- Provide channels for citizens to report privacy
- violations.

Responsible Party:

Governments to create and fund oversight bodies, Civil society to advocate for and participate in these mechanisms, International organizations to provide technical and financial support.

Impact:

- Enhances transparency and accountability in the deployment of surveillance technologies.
- Ensures that surveillance measures align with democratic principles.
- Prevents overreach by state and private entities.

Recommendation 3: Promote Public Awareness and Digital Literacy

Action Needed:

Implement public education campaigns to raise awareness of surveillance technologies, individual privacy rights, and the risks to democracy. These campaigns should target:

- Vulnerable groups, including marginalized communities and activists.
- Youth and civil society actors.

Responsible Party:

- Civil society organizations and educational institutions.
- Governments and regulators.
- Private tech companies as part of their corporate social responsibility.

Impact:

- Empowers citizens to advocate for their privacy rights.
- Strengthens public demand for accountability in surveillance practices.
- Encourages civic engagement in shaping democratic norms.

Recommendation 6: Equip Civil Society with Tools to Monitor and Challenge Surveillance Practices

Action Needed:

- Provide funding, technical resources, and training to civil society organizations (CSOs) to:
- Monitor and report on the misuse of surveillance technologies.
- Advocate for stronger privacy protections.
- Engage in litigation to challenge unlawful surveillance.

Responsible Party:
International donors and NGOs, Governments to create enabling legal environments, CSOs to lead advocacy and monitoring efforts.

Impact:
- Strengthens the capacity of civil society to act as a watchdog for privacy and democratic governance.
- Ensures diverse voices are included in surveillance policy discussions.
- Protects activists, journalists, and marginalized communities from surveillance abuses.

6TH PRIVACY SYMPOSIUM AFRICA

CONCLUSION

The 6th Privacy Symposium Africa (PSA) presents a critical opportunity for Africa to lead the charge in redefining privacy and data protection practices to align with its unique societal, technological, and policy dynamics. Through the 2024 theme, "Bridging Policy, Technology, and Societal Dynamics," PSA emphasizes the need for a multi-stakeholder approach to tackling challenges in privacy governance while promoting inclusivity, equity, and innovation.

The key policy recommendations put forward in this document align with PSA's objectives and build on the momentum generated by the symposium's initiatives, including master classes, sector-specific discussions, and critical insights from the Privacy Scorecard Report. These recommendations aim to address key gaps and provide actionable solutions in areas such as Election Data Governance, AI regulation, sector-specific privacy frameworks, and cross-border privacy collaboration.

Organized by: UNWANTED WITNESS · Law Society of Zimbabwe · MISA ZIMBABWE

In partnership with: Hewlett Foundation · PRIVACY INTERNATIONAL · CIVIL RIGHTS DEFENDERS · OPEN SOCIETY FOUNDATIONS · accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

6TH PRIVACY SYMPOSIUM AFRICA

CALL TO ACTION

To advance data protection and privacy across the continent, we call upon all stakeholders to act collectively and decisively.

a. Governments and Policymakers are urged to adopt and implement robust, enforceable legal frameworks that ensure the protection of personal data, particularly in high-risk sectors such as electoral processes, healthcare, and financial services. They must work towards harmonizing regulations across jurisdictions to enhance cross-border collaboration and trust.

b. Civil Society Organizations are encouraged to sustain advocacy efforts, raising public awareness about privacy rights while holding institutions accountable for data protection breaches.

c. Private Sector Actors must integrate privacy-by-design principles into their business models, embracing transparency and ethical practices in data collection, storage, and usage to build consumer trust.

d. Academics and Researchers should prioritize studies on emerging challenges in data protection, offering evidence-based insights to guide policy decisions and regulatory interventions.

e. Data Protection Regulators must establish proactive enforcement strategies, streamline compliance requirements, and foster partnerships with industry and civil society to address regulatory gaps and emerging threats.

f. The General Public is encouraged to actively participate in privacy conversations, stay informed of their rights, and hold institutions accountable for protecting their personal data.

Organized by: UNWANTED WITNESS · Law Society of Zimbabwe · MISA ZIMBABWE

In partnership with: Hewlett Foundation · PRIVACY INTERNATIONAL · CIVIL RIGHTS DEFENDERS · OPEN SOCIETY FOUNDATIONS · accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

6TH PRIVACY SYMPOSIUM AFRICA

A COLLABORATIVE PATH FORWARD

Privacy and data protection are not just legal imperatives but moral obligations that touch every aspect of our lives. The African continent, with its growing digital economy and diverse societal landscape, has the potential to pioneer solutions that are both innovative and equitable.

The Unwanted Witness reiterates its commitment to convening diverse voices and perspectives, fostering dialogue, and championing initiatives that empower individuals and communities to safeguard their privacy. Together, we can build an Africa where technology and privacy coexist harmoniously, fostering growth while upholding the dignity and rights of all.

Let us act now, collectively and decisively, to make privacy a cornerstone of Africa's digital future.

Organized by: Unwanted Witness · Law Society of Zimbabwe · MISA Zimbabwe

In partnership with: Hewlett Foundation · Privacy International · Civil Rights Defenders · Open Society Foundations · accountabilitylab Zimbabwe

For more information: www.privacysymposiumafrica.com

APPENDIX:

Full agenda of the 6th PSA.

PROGRAM DAY ONE

Tuesday 19th November, 2024

8:30 am - 9:45 am
Master Class (For Lawyers)

10:00 am - 10:10 am
Opening Ceremony

10:10 am - 10:20 am
Speech by the Minister of ICT

10:20 am -11:25 am
Panel 1: Exploring Global Perspectives on AI Regulation in Data Protection and Extracting Lessons for Africa Amidst Weak Legal Frameworks.

11:25 am -11:30 am
Interlude

11:30 am - 12:30 pm
Panel 2: Harnessing the power of AI – What does it mean to the concept of humanity by MISA

12:30 pm - 1:30 pm
The Unwanted Witness Privacy Moot Court Competition 2024: Overall Champion Experience

1:30 pm - 2:00 pm
Lunch Break

2:05 pm - 3:20 pm
Panel 3: Privacy in the Age of Social Media: Are We All Oversharing?

3:30 pm - 4:30 pm
Women in Privacy "One-on-One"

4:35 pm – 5:00 pm
POTRAZ/HIT/DPO graduation ceremony

5:05 pm
End

Organized by: UNWANTED WITNESS · Law Society of Zimbabwe · MISA ZIMBABWE

In partnership with: Hewlett Foundation · PRIVACY INTERNATIONAL · CIVIL RIGHTS DEFENDERS · OPEN SOCIETY FOUNDATIONS · accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

Full agenda of the 6th

PROGRAM DAY TWO

Wednesday 20th November, 2024

8:30 am - 9:45 am
Master Class (Finance and Banking)

10:00 am - 10:10 am
Key Note Address/Law Society President

10:10 am - 10:30 am
Zimbabwe Data Protection Regulations Launch

10:35 am - 11:45 am

Panel 4: Surveillance, Privacy, and the Future of Democracy in Africa

11:45 am - 11:50 am
Interlude

11:45 am - 12:55 pm

Panel 5: Complexities of Election Data Management in Africa's Digital Democracy: Challenges and Opportunities.

12:55 pm - 1:30 pm
Lunch Break

1:30 pm -2:45 pm

Let's Talk: Let's Talk – Data Protection and Elections in Africa

2:50 pm - 3:50 pm

Panel 6: Strengthening Data Privacy and Protection in Zimbabwe: Examining the Gaps, Challenges, and Pathways to Accountability by Accountability lab

4:00 pm - 4:05 pm
Interlude

4:05 pm - 5:05 pm

Panel 7: Privacy Mishaps: Funny Stories from the Workplace

5:10 pm
End

Organized by: UNWANTED WITNESS · Law Society of Zimbabwe · MISA ZIMBABWE

In partnership with: Hewlett Foundation · PRIVACY INTERNATIONAL · CIVIL RIGHTS DEFENDERS · OPEN SOCIETY FOUNDATIONS · accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

Full agenda of the 6th PSA.

PROGRAM DAY THREE

Thursday 21st November, 2024

9:00 am - 9:25 pm
Key Note Address/Minister for Justice Legal and Parliamentary Affairs

9:30 am - 11:00 am

Panel 8: Data Breach Preparedness and Response: Mitigating Risks and Restoring Trust in Financial Institutions.

11:05 am – 11:25 am

Paper Presentation

11:30 pm -12:40 pm

Panel 9: (Conversation with Regulators): Proactive vs. Reactive Enforcement Strategies: Maximizing Impact in Data Protection Regulation

12:40 pm -2:00 pm

Lunch Break

2:20 pm - 2:30 pm

4th Privacy Scorecard Report presentation and Launch

2:30 pm - 3:50 pm

Panel 10: Law Society of Zimbabwe

3:50 pm - 4:00 pm

Remarks from UW

4:00 pm - 4:10 pm

Report Launch (Closing remarks)

4:15 pm

End

Organized by: UNWANTED WITNESS, Law Society of Zimbabwe, MISA ZIMBABWE

In partnership with: Hewlett Foundation, PRIVACY INTERNATIONAL, CIVIL RIGHTS DEFENDERS, OPEN SOCIETY FOUNDATIONS, accountabilitylab ZIMBABWE

For more information: www.privacysymposiumafrica.com

6TH PRIVACY SYMPOSIUM AFRICA

6th Privacy Symposium Africa Panelists.

Panel	Panelists
Exploring Global Perspectives on AI Regulation in Data Protection and Extracting Lessons for Africa Amidst Weak Legal Frame works	1. Dr Melody Musoni, PhD | Digital and AI Governance| Founder - Nkosana Maphosa |Law 2. Rutendo Mugadza Mugwagwa | Founder/CEO @ Zimbabwe Innovation and Legal Technology Association | Intellectual Property And Legal Technology. 3. Edith Utete |Child Online Safety | Digital Wellbeing Advocate | Attorney 4. Cornelia Kutterer | Managing Director @Considerati | AI governance research @MIAI-UGA Chair of AI Regulation | Speaker | public affairs, tech policy, data & AI compliance | leading with empathy | bridging data science & law.
Surveillance, Privacy, and the Future of Democracy in Africa	1. Evan Summers |Program Director | National Democratic Institute for International Affairs (NDI) 2. Brian Tinashe Katsidzira |Human Rights & Democracy| Active Citizenship | Tax Justice | Natural Resource Governance | Climate & Ecological Justice | Diversity & Inclusion | Peace,Governance & Policy Development | MSc/ BSc/ LLB 3. Lisa Poggiali |Senior Democracy, Data and Technology Specialist| USAID 4. Josie Thum | Advocacy Officer | Privacy International 5. Innocent Tinashe Chingarande | Associate Partner | Chasi Maguwudze Legal Practice and a registered Legal Practitioner 6. Christopher Musodza |Co-founder and Executive Director | Fungai Africa 7. Tawanda Mugari | Co-Founder & Geek in Chief at Digital Society of Africa | Civic Space Fellow | Ford Foundation Global Fellowship Alumnus
Complexities of Election Data Management in Africa's Digital Democracy: Challenges and Opportunities	1. Mrs Farisai Chaniwa- Director, Media Monitors-Zimbabwe 2. McDonald Lewanika - Regional Director for South and East Africa | Accountability Lab 3. Ed Geraghty | Senior Technologist | Privacy International 4. David Mburu | Democratic Governance and Rule of Law Programme Lead | ICJ-Kenya 5. Melissa Chasi| Data Protection Officer| Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)

6TH PRIVACY SYMPOSIUM AFRICA

6th Privacy Symposium Africa Panelists.

Panel	Panelists
Let's Talk: Data Protection and Elections in Africa	1. Ms. Lilian B. Mahiri-Zaja |Constitutional Law and Governance Expert.
Women in Privacy One on One: Celebrating Achievements, Sharing Experiences, and Inspiring Future Leaders	1. Amaka Ibeji, FIP, CIPM, CIPP/E, CISSP
Privacy Mishaps: Funny Stories from the Workplace	1. Tadzie Madzima | Marketing Leader | Global Communications and Partnerships Expert | Mandela Washington Fellow | JCI's Top Young Person | Resilient Team Leader | Brand Invigorator | DE&I Advocate | Coach & Mentor 2. Desmond Israel ESQ | Empowering Businesses with Next-Level Cybersecurity Solutions | Legal Expert in Data Privacy + Technology | Educator & Researcher 3. Dr Pieter van der Walt (CIPM, MDQM) |Group Chief Privacy Officer at Discovery Limited 4. Rufaro Mhandu | Managing Partner | R. Mhandu Attorneys 5. Mythel Esther Mabika | Deputy Chair | Privacy Practitioners Association (Zimbabwe)
Privacy in the Age of Social Media: Are We All Oversharing?	1. Oladotun (Olaitan) Owoyemi, CIPP/E Privacy Counsel|| Data Protection | 2. Regulatory Intelligence | Digital Health 3. Shanée R. Banda | Communications Officer @ ADRA Zimbabwe | Digital Strategist| Blogger| Writer| Budding Poet 4. Julie Owono | Internet Without Borders 5. Michael Michie |Artifical Intelligence | Technology | Cybersecurity | Video Games | Mental Health | Top 40 under 40 Kenya 2019 | Mentor 6. Janet Machuka |Social Media Brand & Campaign Strategist, SMM Trainer |Founder ATC Digital Academy 7. Melissa Chasi| Data Protection Officer| Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) 8. Salome Nzuma | Communications Specialist

6TH PRIVACY SYMPOSIUM AFRICA

6th Privacy Symposium Africa Panelists.

Panel	Panelists
Data Breach Preparedness and Response: Mitigating Risks and Restoring Trust in Financial Institutions	1. Livhuwani Maswielelo, Regional Privacy Officer – PayU Africa 2. Rosemary Koech-Kimwatu | Lawyer , IVLP 2023, Data Protection, Public Policy- 35 Most Influential Women in Tech (CIO Africa), Africa's Leading Women in Legal Innovation (Africa Law Tech) ILTA Influential Women in Tech 2021 3. Mutsa Mabhande|Group Head IS Security, Governance & Compliance at CBZ Holdings | Harare, Zimbabwe 4. Lori Baker | |Fellow of Information Privacy (FIP) (CIPP-E, CIPT) - VP of DP (for DIFC Commissioner) & Regulatory Compliance; Editorial Boards: DIFC Academy, Journal of Data Protection & Privacy. Views are mine and not of DIFCA. 5. Gilbert Ouko CISA, SCS, RCS, CRC, CCFC | | Head of Compliance and Risk | Conduct Risk | Sanctions Risk | Regulatory Compliance | FCC | AML | Virtual Assets Compliance. 6. Charles Otiang`a Owiti -LL.B, CMILT, ACIArb, MIoD (Kenya)View Charles Otiang`a Owiti -LL.B, CMILT, ACIArb, MIoD (Kenya) |Partner |Legal Consultant Transport & Maritime Law| Advocate| Data Protection (DPIA) Expert| Patent Agent|ICT Mentor |Nairobi County, Kenya 7. Kelvin Sabao |Advocate | Titan Law, Zimbabwe
(Conversation with Regulators): Proactive vs. Reactive Enforcement Strategies: Maximizing Impact	1. Emmanuel Lameck Mkilia| Director General |Personal Data Protection Commission- Tanzania 2. Pille Lehis | Director General |Estonian Data Protection Inspectorate 3. Commissioner Likando Lyuwa | The Office of the Data Protection Commissioner 4. Ms. Tsitsi Mariwo -Director Data Protection | Postal and Telecommunication Regulatory Authority of Zimbabwe (POTRAZ). 5. Ms. Lindokuhle Sibandze | Data Protection Officer at the Eswatini Data Protection Authority

6TH PRIVACY SYMPOSIUM AFRICA

6th Privacy Symposium Africa Panelists.

Panel	Panelists
Strengthening Data Privacy and Protection in Zimbabwe: Examining the Gaps, Challenges, and Pathways to Accountability by Accountability lab	1. Ms. Tsitsi Mariwo -Director Data Protection | Postal and Telecommunication Regulatory Authority of Zimbabwe (POTRAZ). 2. Bridgette Ndlovu – Partnerships and Engagement Officer - Paradigm Initiative 3. Christopher Mhike- Partner at Atherstone & Cook 4. Bridget Mafusire (ISLP) - Deputy Legal Advisor | Ministry of Industry and Commerce
Harnessing the power of AI – What does it mean to the concept of humanity by MISA	1. Nqaba Matshazi | Regional Campaigns Coordinator| MISA 2. Sean Ndlovu | Co-founder and product manager at the Centre for Innovation and Technology – Zimbabwe 3. Arnold Mutasa | Tech lead at FinGenie Consultancy - Zimbabwe