

Guidelines on data access for key stakeholders in African elections

Kwami Ahiabenu



Workshop 17
17 Dock Road
V&A Waterfront
Cape Town, 8001
Cape Town, South Africa
Phone: +27 21 447 6332
Fax: +27 21 447 9529
www.researchictafrica.net

Acknowledgements

Author: **Kwami Ahiabenu**

Research review: **Guy Berger, Liz Orembo**

Project manager: **Naila Govan-Vassen**

Copyeditor: **Helen Walne**

Proofreader: **Drew Haller**

Project: *Data Access for Tech Accountability and Electoral Integrity in Africa* project is funded by Collaboration on ICT Policies East and Central Africa (CIPESA).

Citation: Ahiabenu, K., (2025) *Guidelines on data access for key stakeholders in African elections*. Cape Town: Research ICT Africa

Copyright

Guidelines on data access for key stakeholders in African elections © 2025 by Kwami Ahiabenu is licensed under [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) 

First published by Research ICT Africa in April 2025.

Publisher

Research ICT Africa

Workshop 17

17 Dock Road

Cape Town

South Africa

8001

+27 21 447 6332

info@researchictafrica.net

www.researchictafrica.net

Table of contents

Acknowledgements	1
Executive Summary	3
1. Introduction	4
1.1. Objectives	
2. Recommendations for improving data transparency and accountability	
3. Literature review	5
3.1. The importance of data in elections	5
3.2. Challenges to data access and use	5
3.3. The role of technology and Big Tech	6
3.4. Addressing the data deficit	6
4. Methodology	7
5. Findings and discussions	7
5.1. Key findings from stakeholder input	7
5.2. Data access comparisons between countries	11
5.3. Big Tech and Big Data	12
5.4. Legal and regulatory environment	14
5.5. Common challenges in data access and utilisation	15
6. Conclusion	16
7. Guidelines	
7.1 Elements of guidelines	18
7.2 Implementation advisory: access to data, elections and African standards	19
7.2.1 Implementation guidelines for EMBs on data access	19
7.2.2 Implementation guidance for political actors (parties, groups and independent candidates) on access to data in relation to elections	22
7.2.3 Implementation guidance for civil society on data access and elections	25
8. References	27
Appendices	27

Executive Summary

Access to credible, accurate and transparent electoral data ensures election integrity and strengthens African electoral processes. Recognising this, the [African Alliance for Access to Data](#) (AAAD), with support from the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) and Research ICT Africa (RIA), commissioned this action research to develop guidelines that improve data access for key stakeholders, including Election Management Bodies (EMBs), political actors, civil society organisations and the media.

The study provides three sets of guidelines for EMBs, political actors and civil society in light of the role of data (both public and private) as increasingly relevant to elections. Data informs decisions—whether automated by algorithms or made by humans—and is the fuel of machine-learning Artificial Intelligence (AI). Access to data should incorporate issues of privacy, storage, security, ethical use and sharing.

This research builds on AAAD's Implementation Advisory, informed by African normative frameworks such as the African Union (AU) Data Governance Framework, to refine and finalise data access guidelines. These frameworks, and the resultant guidelines, collectively promote digital governance, freedom of expression, access to information, human rights, non-discrimination and ethical media practices, particularly in the context of elections and digital platforms.

The study involved extensive stakeholder consultations, including face-to-face and virtual interviews with 16 interviewees from Nigeria, Sierra Leone, The Gambia, South Africa, Zimbabwe, Ghana, Senegal and Tanzania. Participants included members of parliament, electoral support organisations, fact-checkers, researchers, journalists, EMB representatives and civil society organisations. Insights were also gathered from engagements at relevant events, such as the African School of Internet Governance (AfriSIG) 2024 in Addis Ababa, and the 2024 Africa Facts Summit and the Coalition Meeting of Stakeholders to Combat Disinformation, both held in Accra.

Findings highlight significant challenges in electoral data access, including unstructured data collection, lack of transparency in campaign finance records, data manipulation risks and disparities in data availability. While digital voter registration has improved accessibility, inconsistencies persist between national and local data sets. Fact-checkers emphasise the need for timely access to reliable data to counter misinformation and disinformation. Emerging technologies, such as AI, hold potential for data verification but are in early adoption stages.

To address these challenges, this study proposes key recommendations. These include implementing open data principles, promoting proactive data disclosure, improving EMB data management, enhancing stakeholder collaboration, safeguarding data integrity, supporting capacity building in data literacy and strengthening legal frameworks to balance transparency with privacy concerns. Effective dissemination and adoption of these guidelines, alongside sustained engagement and partnerships, are crucial to fostering data-driven election integrity across Africa.

1. Introduction

The AAAD, framed within African normative frameworks, including the AU Data Governance Framework, has developed a preliminary implementation advisory for access to data relevant to election integrity. The advisory targets three stakeholder groups: African EMBs, political actors and civil society, including the media.

African researchers and the African electorate are also expected to benefit from this work.

With the support of CIPESA, RIA commissioned action research to develop, refine and finalise a set of specific guidelines to support the three stakeholders in navigating access to electoral data to enhance election integrity.

An elections data ecosystem can be described as an interconnected network of stakeholders, processes, technologies and policies that enable the creation, management, sharing and use of data (RIA, 2024). The ecosystem could comprise data creators, data handlers (processors and managers), data requestors (users), data intermediaries and data governance bodies. The use of technology and infrastructure, data security and privacy, data collaboration mechanisms, and data policies and frameworks would help to create enabling environments for data ecosystems to thrive. Understanding data ecosystems is important to ensure elections data integrity.

There is also a need for requisite collaboration and coordination of elections data elements to ensure data is created, managed, shared and used effectively, ethically and securely. Each element plays a critical role in maintaining the integrity and functionality of the ecosystem. Therefore, effective stakeholder collaboration within a framework of dynamic guidelines can help strengthen election integrity. In most cases, beyond internet companies and political parties, data holders are typically a public entity that may or may not be distinct from government. By virtue of the prescripts of the laws that govern their existence, they are obligated to make data available and accessible under a given condition.

The table below shows a summary of key action points and opportunities for each of the three stakeholders.

Table 1: Action points and opportunities for each stakeholder

Action points/opportunities for civil society	Action points/opportunities for EMBs	Action points/opportunities for political actors
---	--------------------------------------	--

<ul style="list-style-type: none"> • Monitor • Collaborate • Promote accountability 	<ul style="list-style-type: none"> • Demand disclosure from social media • Enable partnerships to monitor • Communicate the results 	<ul style="list-style-type: none"> • Transparency • Empower multistakeholder efforts • Keep it clean
--	--	---

Following the introduction, the report covers the stakeholder engagement findings, guidelines, conclusion and relevant appendices, including a proposed plan for disseminating the guidelines to ensure its adoption. (See Appendix 1 for publicity plan.)

1.1 Objectives

The objectives of the study are:

1. To identify the challenges faced by election stakeholders (EMBs, political parties, media outlets and civil society organisations) in accessing and using election-related data.
2. To gather insights on best practices for ensuring data transparency, accuracy and accessibility in the electoral process.
3. To develop and finalise data access guidelines that are aligned with African normative frameworks and support the effective use of data to strengthen election integrity.

2. Recommendation for improving data transparency and accountability

To enhance data transparency and accountability, stakeholders have proposed the following guidelines:

- **Leverage African normative frameworks:** Use African normative frameworks as guiding principles to enhance data access and availability across the continent.
- **Implement open data principles:** Adopt the principles of open data, the Open Government Partnership and relevant African standards across countries to improve access to credible election and social data.
- **Promote electoral transparency:** Ensure transparency in data availability and the electoral process to build public trust.
- **Support Big Data management:** Provide technical and financial assistance to national bodies for effective data collection, processing and dissemination.
- **Encourage proactive data sharing:** Data holders should proactively share detailed data with the public, especially on their websites or relevant online platforms, to foster greater acceptance of, and trust in, the information provided.
- **Clarify data restrictions:** Clearly reasons for withholding data, especially when related to national security, privacy or public safety concerns.

- **Enhance transparency mechanisms:** Authorities must take extra steps to enhance data transparency, as perceived opacity can erode public trust even when there is nothing to hide.
- **Ensure disaggregated data:** Provide disaggregated data to increase its credibility, making it more acceptable and trustworthy to users.
- **Safeguard data integrity in the age of AI:** Invest in mechanisms to protect data from manipulation during creation, processing and storage, while enabling easy verification of information and sources.
- **Monitor AI usage:** Be proactive in exploring AI's potential while implementing safeguards against its misuse and associated risks, such as its use in creating misinformation and disinformation.
- **Timely and accessible data dissemination:** Ensure data is disseminated promptly, made available online, and that the public is aware of data sources and opportunities.
- **Promote multilingual accessibility:** Make data available in local languages to improve accessibility for diverse populations.
- **Adopt a human rights-centred approach:** Anchor data guidelines in human rights principles to foster greater participation and inclusivity.
- **Simplify guidelines:** Ensure guidelines are concise, clear and free of technical jargon to be relevant to a wide range of stakeholders.
- **Respect national sovereignty:** Draft guidelines that respect the sovereignty of individual countries, avoiding provisions that infringe on national autonomy.
- **Integrate multiple data types:** Work towards integrating diverse data sources to avoid silos, which hinder accessibility and usability.
- **Strengthen data-holding institutions:** Provide training, resources and capacity-building support to data-holding institutions to improve the seamless availability of data.

According to stakeholders, these recommendations can create a more transparent, accountable and inclusive data ecosystem that supports informed decision-making and data integrity, particularly in electoral contexts.

3. Literature review

The integrity of electoral processes is fundamental to democratic governance. A key component of this integrity lies in the accessibility and effective use of election-related data. This literature review examines the critical role of data access in strengthening elections, exploring the challenges stakeholders face and highlighting potential solutions. The review draws on insights from scholars and organisations working in the field of election observation, data analysis and democratic development.

3.1 The importance of data in elections

Elections often fail to meet democratic ideals due to electoral malpractice, including the manipulation of rules, voter preferences and voting processes. The likelihood of such misconduct is influenced by the costs faced by political actors and the scarcity of reliable electoral data. Strengthening monitoring mechanisms and improving access to credible electoral data can raise the costs of manipulation and help deter malpractice (Birch, 2013). Elections are data-driven processes. Data forms the backbone of every stage, from voter registration and polling station management to results tabulation and analysis. As highlighted in the preceding report, stakeholders need diverse data types, including voter rolls, polling station locations, election results and campaign finance information to effectively participate in and scrutinise electoral processes. Data transparency fosters trust in elections, enabling citizens, political parties and civil society organisations to verify the legitimacy of outcomes and hold electoral bodies accountable (Norris, 2014). Conversely, restricted access to data breeds suspicion, fuelling electoral disputes and undermining public confidence in democratic institutions (Norris, 2014). As emphasised by International IDEA (2022), electoral disputes frequently stem from challenges in results management and voter registration, underscoring the crucial need for data integrity in these areas. Furthermore, around the world, many voters lack access to vital information about politicians, public services and government performance, which undermines democratic accountability. The widespread knowledge deficit hinders voters' ability to elect competent leaders and hold them accountable, leading to poor governance and increased risk of corruption. A functioning democracy depends on an informed electorate, but without access to reliable information, voters are unable to make sound choices and politicians face little pressure to act in the public's interest (Dunning et al., 2019).

3.2 Challenges to data access and use

Despite the recognised importance of data, stakeholders often encounter significant obstacles in accessing and using it effectively. This report highlights key challenges, including a lack of structured data management mechanisms, the prevalence of unstructured data and the absence of clear guidelines for data use. Many electoral bodies struggle with outdated paper-based systems, which hinders efficient data retrieval and analysis (Reilly, 2018). As noted by the interviewees, the multiplicity of data silos across different government agencies further complicates data integration and validation. Moreover, legal frameworks governing data access vary considerably across countries, with some nations lacking robust data protection laws and others imposing restrictions that impede transparency (Gadasu, 2024). The report's findings echo concerns about the manipulation of data during its transmission, the selective release of partial results and the existence of parallel data systems within electoral bodies, all of which pose serious threats to election integrity.

3.3 The role of technology and Big Tech

The rise of digital technologies has transformed the electoral landscape, presenting opportunities and challenges. While digitalisation can enhance data management and accessibility, it also introduces new risks, such as cybersecurity threats and the potential for data breaches (Alvarez & Hall, 2010). The increasing influence of social media platforms in electoral communication necessitates a closer examination of their role in shaping public discourse and disseminating information. Big Tech companies hold vast amounts of user data that can be leveraged for political advertising and voter targeting. The lack of transparency surrounding data collection and usage by these platforms raises concerns about potential manipulation and undue influence on electoral outcomes (Borgesius et al., 2018).

3.4 Addressing the data deficit

Improving data access and utilisation requires a multifaceted approach. First, electoral bodies must prioritise the modernisation of their data management systems, transitioning from paper-based processes to robust digital platforms. This includes investing in data infrastructure, developing standardised data protocols and ensuring the security and integrity of electoral data. Second, legal frameworks governing data access should be strengthened to promote transparency and accountability. This involves enacting clear guidelines for data release, protecting personal information and establishing mechanisms for enforcing data access rights. Third, capacity-building initiatives are essential to equip stakeholders with the skills and knowledge to effectively analyse and interpret electoral data. This includes training programmes on data science, social media mining and AI, as well as promoting data literacy among citizens and civil society organisations. Fourth, fostering collaboration between electoral bodies, civil society organisations and international actors is crucial for sharing best practices and promoting data transparency. Adhering to established normative frameworks, such as those developed by the AU and the Association of African Election Authorities (2024) can provide valuable guidance for enhancing data access and election integrity. Finally, addressing the challenges posed by Big Tech requires a concerted effort to promote transparency and accountability in the digital sphere. This may involve regulating social media platforms, establishing clear guidelines for political advertising and empowering citizens to critically evaluate online information.

4. Methodology

This research employs a qualitative approach to develop, refine and finalise data access guidelines aimed at supporting EMBs, political parties, media outlets and civil society organisations in leveraging data to enhance election integrity. A comprehensive consultation process was undertaken to ensure the guidelines are tailored to stakeholder needs.

A series of stakeholder consultations were conducted to identify challenges related to election data access and use and gather insights on best practices for promoting transparency, accuracy and accessibility. These consultations ensured that the guidelines align with African normative frameworks and address practical concerns in election-related data management.

Data collection involved direct engagement with stakeholders through a combination of face-to-face and virtual interviews. A total of 16 interviewees participated, representing a diverse range of countries across Africa, including Nigeria, Sierra Leone, The Gambia, South Africa, Zimbabwe, Ghana, Senegal and Tanzania. The interviewees included fact-checkers, members of parliament, electoral support non-governmental organisations (NGOs), researchers, journalists, EMB representatives and civil society organisations. See Appendix 2 for a list of participants.

In addition to individual interviews, researchers engaged with stakeholders at three key events: the AfriSIG 2024 in Addis Ababa, the 2024 Africa Facts Summit in Accra, and a meeting of the Coalition of Stakeholders to Combat Disinformation, also in Accra. These stakeholders were involved in various activities, including fact-checking, media literacy training, resilience building to combat misinformation and efforts to debunk or pre-bunk disinformation to ensure the integrity of electoral data.

5. Findings and discussions

5.1 Key findings from stakeholder input

Data is a critical component of any election, as electoral processes and election management systems rely on data and information. Most of the interviewees make use of data, however, the majority lacked structured mechanisms for managing and interacting with it. Most work with unstructured data without written guidelines for its use, creation and application. Stakeholders cited electoral data types that vary from country to country. These included data on voters' rolls; voting and registration sites; election results; polls; geographical location of polling stations; voters by age; voting patterns; candidates; number of temporary electoral workers; past elections; electoral violence; voter turnout; campaign financing for political parties and candidates; new-voter registration numbers; and demographics of a country through census information. Census data is vitally important because it serves as a quantifying benchmark to compare voters' rolls to estimated eligible voters.

Data analysis can help us understand voting trends, patterns, data and information flow, and the impact of misinformation on election integrity. However, campaign finance data remains largely inaccessible, with many political parties and candidates failing to disclose financial records despite legal mandates.

5.1.1 Data is central to elections

One respondent emphasised the importance of data in fact-checking, stating:

“Okay, so I think data is very, very important in the work we do as fact-checkers. In fact, as we're going to cover elections, we need to understand election violence hotspots. That is a piece of data.

We need to find out the number of people who are offline and who are online. All of these are pieces of data that inform us and the strategy to use, to be able to do fact check effectively. So, our election coverage is heavy on data”.

Given that election coverage is heavily reliant on data, some interviewees highlighted the use of surveys to generate insights that inform fact-checking strategies. Fact-checkers expressed a strong interest in understanding the extent of disinformation at different stages of the electoral process and exploring effective ways to access reliable data to counter misinformation.

Ensuring data integrity fosters transparency and trust, which are two essential pillars of the electoral process. As one respondent noted, maintaining robust data systems is fundamental to upholding the credibility and fairness of elections.

“Elections today in Africa … well, not just in Africa because our recent Global State of Democracy report shows that globally most electoral outcomes are contested, leading to disputes. The whole issue around electoral disputes is because people don’t trust, you know, the processes leading to elections results, so basically that’s where I see the centrality of data.”

In most cases, electoral disputes are primarily associated with challenges in results management and voter registration. Ensuring the integrity of data in these critical areas is essential to maintaining the credibility and transparency of electoral processes (IDEA, 2022). Weaknesses in voter registration systems and inconsistencies in result collation can lead to disputes that undermine public trust in elections (Norris, 2014). As elections data, especially results, travels from polling stations to provincial and constituency level and thereafter to national level, some stakeholders noted that data might be manipulated en route. Some EMBs release elections result only at national level, but there is no disaggregated data at provincial, constituency or polling-station levels. Results at local wards/councils or polling stations cannot be changed because they are announced at community level. For example, Parliament results are difficult to change, but there are reported cases of presidential results being changed at the national collation level, which creates data integrity issues.

Another type of data required during elections is political parties’ manifestos, in which there are usually a lot of claims (for example, the number of roads, hospitals and schools built). Verifying these claims requires a lot of work and this type of information is not available in all countries. Some countries have digitalised the voter register, which makes it possible in principle to share data with relevant stakeholders such as political parties. Some of these voter registers also incorporate a Biometric Verification System that automates, validates and confirms that a voter is a member of the polling station, which ensures confidence in the system. This also ensures that a polling station cannot record more votes than the number of voters registered there. In addition, some political parties now keep electronic databases of their members, which creates a data stream.

Data access is one of panaceas to the dissemination of misinformation, as it can be used to counter rumours or distorted information and helps voters make sound decisions.

“It behooves institutions who are trustees of that data to make those data available to citizens as quickly and as easily as possible in order for them to make informed election decisions,” another respondent stated.

5.1.2 Data access and electoral integrity

Accessing data should be as easy as possible to help people avoid skewed information. Data results in awareness and enables people to make quality decisions informed by evidence (African Alliance on Access to Data(AAAD), 2024). Thus, the quality of data and its availability is paramount, as one respondent mentioned.

“Just make it available to the citizens. If you are a public official, the data and information in your custody is not for you to keep. It is for you to make it available to people so they will be able to make quality decisions from those data that you have. So, my only suggestion is for public office holders to, as much as possible, make that information available to people.”

Electoral data can have different functions. For example, some facilitate participation, and others promote transparency and trust. All aspects have associated challenges in terms of access. Transparency, security and accuracy of electoral data is key. It is important to encourage data holders to be more proactive in disclosing the information —for example, by regularly updating the data on their websites. In addition, data holders must strive to understand the data needs of different election stakeholders so they can meet these.

Data quality is key: the better the quality of the data, the better choices people will make. Speed is also an important component of today’s information ecosystems.

At the same time, it is important to ensure the integrity of information being accessed by various players. The way data is harvested, stored, processed and distributed is key to its availability within the dispensation of legal and regulatory environments. For example, a data holder could argue that they cannot release data due to their inability to redact private and personal information, whereas a robust system can easily negate this.

According to most electoral laws, access to data is meant to be easy (Open Elections Data Initiative, 2024). However, it can be practically difficult to access data from some EMBs. There have been several reported cases of some stakeholders resorting to courts to force EMBs to give them information. The release of data or information is guided by an established protocol. For example, in some countries it is illegal to divulge personal information, and entities must redact personal information to avoid compromising the privacy of individuals in line with legal protocols.

Overall, the interviewees noted an improvement in the availability of data across most areas, however, there is still much work to be done. They suggested that most of the data they use is found on data holders’ websites, though sometimes it is not in a usable format. Beyond what is available on websites, requests are made directly to data holders for the release of information.

Interviewees said access to data is not standardised since it differs from country to country, based on legal frameworks. Access to election data is easier in countries that have strong data protection guidelines and laws than countries that do not have such provisions. The availability of data from private entities, such as Big Tech, also varies from country to country. However, most interviewees noted that it is becoming difficult to access data from Big Tech companies across the continent. Also, different countries have different levels of privacy protection. For example, in Nigeria, an embassy can access the bank balance of a visa applicant whereas in South Africa they cannot. This reflects the different levels of data protection laws in different countries, which then affects how data holders in the electoral process also interact with data.

There are several options to ensure a data and information ecosystem that supports elections data integrity effectively. A respondent noted:

“A starting-point country would do well to subscribe to the established normative framework at the continental Africa level, [which] already has some guidelines as well as protocols pertaining to access to information and freedom of expression.”

The Association of African Election Authorities (AAEA) recently developed principles and guidelines for the use of digital and social media in electoral processes. These guidelines underscore the importance of access to information as a fundamental human right, making it non-negotiable. The Guidelines also under point 11.5 urge that: “Social media operators should provide effective systems of vetted access to data for research purposes as relevant to electoral integrity.” Therefore, it is crucial for countries to implement these provisions to safeguard the integrity of electoral systems (AAEA, 2024).

The concept of ‘Information disorder’ in its various forms can significantly undermine the electoral process. The quality of information directly influences how electorates perceive and accept election outcomes. Ensuring the integrity of electoral data is therefore imperative, as misinformation can skew public trust in election results (IDEA, 2023). To counter this, it is essential to create an environment where accurate and timely information is accessible not only to fact-checkers but also to the media and the public. By making data available, there is an opportunity for misinformation to be nipped in the bud (CIPESA, 2024).

AI emerged as a topic during interviews conducted for this research, with several stakeholders indicating that it is still in the early stages of integration into the electoral data ecosystem. Some countries have begun to experiment with AI, particularly in areas such as data management and analysis, but full integration remains a distant goal. Similarly, some fact-checking organisations, media outlets, civil society groups and political parties are exploring the use of AI, but most stakeholders are still in the initial phases of adopting this technology in the electoral context (Itodo, 2024).

5.1.3 Data access problems

While most EMBs have a mechanism of digital capture of data, these systems are often centralised, limiting access to data for grassroots organisations. In cases where data systems are decentralised, discrepancies often arise between the data provided at the national and local government levels. Some stakeholders reported that data received at national level sometimes conflicts with that captured at ward or polling-station level. These discrepancies can undermine the integrity of the election process and cause confusion among election observers and stakeholders.

Further concerns were raised by some stakeholders about parallel data systems within certain EMBs, where misrepresented data is provided to opposition parties while the government receives accurate data. This practice opens the door to electoral manipulation, as the governing party might use this privileged data to influence outcomes while keeping the opposition in the dark. Additionally, some data holders might alter data for various reasons, increasing the risk of manipulation.

To safeguard the integrity of electoral data, it is crucial to implement systems that protect against tampering and ensure that data is preserved throughout the electoral process. This would help to address many election-related litigation issues, which could otherwise result in prolonged legal battles.

Data is difficult to acquire due to several reasons, including the use of paper-based data systems, an over-reliance on oral means of communication, and a lack of awareness of data availability. There is often no organised repository of data, which results in multiple and disjointed data points. This makes it difficult to access data. The multiplicity of data silos —for example, driving licences, passports, national identity documents (IDs), voter IDs, tax IDs and social security IDs —means there is no single mechanism to validate a voters' register. Thus, harmonisation of all these data points can help in achieving a universal registration, where a user can consume multiple services with only one card. This could result in a robust voter roll, thereby preventing conflict while facilitating the availability of disaggregated voters' data.

One shared concern among the interviewed stakeholders was how to balance privacy and confidentiality with national security concerns. One stakeholder said individuals have a human right to privacy in terms of personal data and personal information. For example, there is an ongoing debate about the release of assets-declaration forms by elected officials, because though they are public officials, they still have privacy and confidentiality rights as individuals.

Stakeholders agreed that there is scant training on the intricacies of handling data and data integrity, and even fewer intentional training courses related to data science, social-media mining and AI. Also, some of the available courses tend to be expensive, putting them out of reach for most stakeholders who are interested in building their capacity. Also, most trainings take place at national or regional level, with only a few at grassroots level.

5.2 Data access comparisons between countries

Interviewees observed significant disparities in data access across countries. One respondent said:

“Very often, there is differences from one country to the next. In my experience, South Africa is far ahead. Other countries do not have an equivalent of this institution or that organisation. Even if they do, these organisations do not have resources and they are understaffed, making access to data difficult.”

There is a significant gap in the experiences of fact-checkers across different African countries, particularly in relation to data access and availability. In some countries, effectively conducting fact-checking is a challenging task due to restricted or unreliable data. One respondent emphasised the difficulty of obtaining information in Nigeria, stating:

“For example, Nigeria is a very difficult place to access information, unless it is already public, whether on institutions like Bank of Nigeria, Central Bank of Nigeria or Independent National Electoral Commission (INEC) website. Then that's great, but if it comes to actual requests for information, that's a lot harder.”

Other interviewees also noted that even basic requests for comments or data are often met with significant barriers, with some institutions providing limited or no access to public records. While there are laws that grant data users the right to access information, the process can be lengthy and success rates vary significantly across countries. Some of the stakeholders said they experienced the use of legal obligations as a barrier to the release of information they requested.

“If they also want to stonewall you and they don't want you to really get that information, they can use a lot of other kind of legal obligations to really slow the process down.”

These challenges highlight the disparities in the effectiveness of fact-checking efforts and the need for more robust data-access mechanisms to support electoral transparency and accountability.

In some countries, extensive electoral data is readily available for analysis, allowing fact-checkers to easily verify claims. In contrast, other countries offer limited or difficult-to-access data sources, leading fact-checkers to rely on expert analysis. One respondent shared:

“And in those cases, we then rely on experts to basically approximate what would be plausible and what would be implausible.”

The lived experience of fact-checkers on the continent is different depending on location. In some countries, data can be easily accessed online by simply entering a URL, while in others, the process is cumbersome. For example, in some regions, fact-checkers must write a formal request letter by hand, mail it, and then wait months for a response. The data received is often in paper form, which then requires digitalisation before it can be used for analysis.

This highlights that not all countries approach data with the same spirit and the same intent. Electoral systems are not uniform, thereby data requirement varies. For example, Sierra Leone changes its voting system each elections cycle, which makes standardisation of data handling difficult.

5.3 Big Tech and Big Data

The advancement in digital technologies has enhanced our capacity to communicate, and when we communicate, we produce data that is harvested by several actors, including social media companies. The question becomes: what are the established protocols for making this data available? Also, the ability to verify data becomes important as there are so many data points. One of the social-media data assets that would be helpful, for example, is the amount of identified false narratives and disinformation taken down during elections. While this data is historic, it can help in understanding the evolution of disinformation tactics.

Social media platforms have become integral to modern election processes. As one respondent noted:

“In fact, the traditional media is no longer as influential. Like the printed newspapers, sometimes radio stations, they are no longer as influential as WhatsApp, TikTok, Facebook or Twitter. That’s where most of the conversations around elections are happening.”

Most voters are turning to social media because they can easily access a lot of electoral information from these channels. When asked if Big Tech can influence electoral outcomes, stakeholders said it is a likely scenario. However, there is no direct evidence linking Big Tech influence on electoral outcomes. One respondent said:

“That I’m not sure of. I think election architecture is robust enough to stand on its own without the external influence of Big Tech.”

Stakeholders interviewed for this research had varied experiences dealing with Big Tech. Some have good working relationships with them that facilitate access to data, but others have struggled to even communicate with big companies such as Meta, X or TikTok. Stakeholders said their colleagues in countries in the West, especially in the European Union (EU), have better responses from Big Tech in comparison to African countries. The explanation is that EU rules and laws help put pressure on Big Tech companies to comply, whereas African countries do not have such regulatory provisions. The interviewees reported diverse relationships with Big Tech, with some in partnership with Facebook to serve as fact-checkers. The data required from Big Tech includes historical trends and sentiments —what are people saying? For example, X trends can pinpoint what people are talking about, and flagged misinformation can alert the fact-checking team to issues that warrant investigation. Some interviewees said they had training sessions with Google on how to use their tools to make accessing information easier. Respondent said that because Big Tech is a large repository of data that is relevant to their work, it is imperative that a pathway be created to access such data.

Interviewees generally agreed that social media is highly influential in elections, with many political actors spending money on advertising as a tactic to get ahead in elections. Therefore, information linked to social media becomes one of the key parameters for stakeholders to seek access. This calls for more advocacy for Big Tech platforms to make relevant data available to aid the work of stakeholders. Interviewees said nurturing relationships with Big Tech helps facilitate the release of data, but because

they are large private companies accountable to shareholders, they are invariably antagonistic and non-proactive. In comparison, public entities are obliged to release data and are accountable to citizens. Thus, Big Tech rarely has responsibility and accountability and has no incentive to share any information. Besides limiting access to data, some Big Tech companies also limit access to some key tools, such as Crowd Tangle, which facilitates analysis of Facebook posts. When such tools or data are available, they have a price tag and the access fees are beyond the financial capacity of most of the stakeholders interviewed.

An interviewee suggested that the pathway of legislation might not be the best approach in dealing with Big Tech:

"I don't think the answer is legislation, but there's got to be a consensus conversation between Africans and Big Tech so that there's some form of transparency accountability in the ways in which Big Tech operates."

Also, when it comes to Big Tech, names like X, Google and Facebook come to mind. However, we must note that tech giants such as MTN might also be assuming characteristics of Big Tech, so there is need to pay attention to them.

5.4 Legal and regulatory environment

Many legal and regulatory provisions can help data seekers access data from data holders. These include electoral laws that mandate EMBs to give credible data to the public. Some countries have constitutional provisions for data to be made available to citizens, and freedom of information laws are also key enablers of information flow to the public. However, stakeholders reported that bureaucratic and administrative hurdles are significant barriers to accessing data and information. A respondent recounted:

"Sometimes it can be extremely difficult to obtain information from the entities supposed to hold it in trust for the people, such as government agencies."

Despite these challenges, there is a consensus among the interviewees that the Right to Information (RTI) has been immensely helpful, though it still has not solved the issues of availability of data for stakeholders. A respondent shared this example:

"In fact, there's an investigation that we did, but for the RTI law, it would have been difficult to get information from the said institution."

Some interviewees noted that some countries use freedom of information laws against opposition due to some provisions that tend to suppress access to data. Ironically, laws that are expected to promote access to information make it even harder. In South Africa, a respondent noted:

"We have the Promotion of Access to Information Act (PAIA) of 2000 that regulates access, public access to government data, official data, so it encourages the public to have access to official data."

And it's a useful tool in South Africa to get people, especially in official capacity, to make data available to the public. So, yeah, generally your access to data is easy and straightforward."

Overall, there are no laws that prevent any institution from providing any information to a data seeker, but they often use security constraints as an excuse. However, even if information is withheld due to a provision of law that deems it security in nature, a justification for the action is expected. Some interviewees noted that their RTI law provides for a given number of days for journalists and fact-checkers to obtain requested information from institutions. However, for fact-checkers and journalists who need the information as quickly as possible, it is frustrating to wait for information amid deadlines. Some stakeholders said it might take three to six months for data to be released, and sometimes the data is only released when the requester goes to court. Some interviewees said that data they had requested to aid their electoral work was only released after the elections.

Interviewees noted that global open-data partnerships and open-data movements have helped to increase data availability. However, individual countries are at various stages of implementation. There is also the cost issue of accessing data online, including the often-prohibitive cost of Internet connections, computers and even basic electricity.

5.5 Common challenges in data access and utilisation

Some stakeholders noted that the discussion of challenges linked to access, availability and usability of election data in Africa cannot be viewed as an island. One respondent noted:

"I don't think governments in Africa have come to the realisation and an understanding of how much data can help with policymaking, for example. But I'm not always sure that our governments are ready to release that information publicly, which is a problem."

This highlights the broader, limited perspective on the role of data in policymaking, which in turn hampers access to election data. There is a common notion that most governments in Africa are not ready to be transparent and therefore do not subscribe to open-access data ideology. This makes it difficult and sometimes impossible to extract requisite data or information from governments across the continent. For example, several countries are slow to release data, which delays the work process of stakeholders. In the case of fact-checking, this could be problematic as speed is essential for stemming the tide of fast-travelling disinformation.

Further, some interviewees indicated that there are resource constraints when it comes to data and information availability. Some countries do not have the budgets necessary for pulling together information to make it available to the public. Some countries do not have content management systems to extract the data and pull it together for the public good. This means there is a data void, which creates problems for stakeholders seeking to access relevant data and information.

Also, most data is not available online, making it difficult to assess or to systematically verify. For example, finding disaggregated data, such as how many men and women cast their ballot during elections, is problematic. There is also a low level of collaboration between data users and requesters to

enable access to data in a timely manner. Coupled with poor data organisation and record-keeping duplication, some data provided is obsolete, which renders some data sets useless or difficult to interpret.

Some EMBs do not have a full complement of staff, such as data scientists, which makes it difficult for them to generate useful data for stakeholders. A lack of training programmes targeting the capacity-building needs of the various EMBs exacerbates matters.

6. Conclusion

This research has highlighted the crucial role of data in maintaining election integrity and identified key areas where access to, management and use of electoral data can be improved. Through consultations with stakeholders across several African countries, including fact-checkers, EMBs, civil society organisations, journalists and researchers, the research identified the challenges and opportunities in ensuring the availability, accuracy and transparency of data in electoral processes.

The key findings reveal that while data plays a crucial role in electoral processes —from voter registration and election results to campaign finance and political party activities —many stakeholders face difficulties in accessing reliable, structured and usable data. A significant number of interviewees indicated that data is often unstructured and lacks standardised guidelines for its use, creation and application, which hinders its effective deployment. While some countries have made strides in digitalising electoral data, the lack of consistency in data availability, particularly across borders, creates disparities in how data is used and accessed.

The consultation process revealed that data types critical for elections, including voter rolls, election results, polls, geographical data and census information, are not always available or easily accessible. Data analysis can provide valuable insights into voting trends, voter behaviour and the impact of misinformation on election outcomes. However, campaign finance data remains largely inaccessible in many countries, with political parties and candidates failing to disclose financial records as required by law. Furthermore, some stakeholders raised concerns about data manipulation, particularly in the aggregation and collation of election results, which undermines public trust in electoral outcomes.

Data integrity is vital for ensuring transparency and trust in electoral systems. Stakeholders highlighted the role of data in combating misinformation and enhancing fact-checking efforts. The need for accessible and accurate data to ensure informed electoral decisions was underscored, with participants emphasising the importance of making data available to the public in a timely, easy-to-understand manner. Interviewees also pointed to the increasing need for training on data science, social media mining and AI in the electoral context, particularly in countries where such training is scarce and costly.

Additionally, the research explored the challenges posed by privacy, national security concerns and the need for data protection, with stakeholders highlighting difficulty in balancing these concerns against the need for open data access. Furthermore, there was a significant variation in data access across

countries, with some nations having well-established frameworks for data release and others remaining entrenched in bureaucratic and legal barriers.

The integration of digital technologies, particularly social media and Big Data has transformed the electoral landscape. While social media platforms provide valuable spaces for election-related information, they also pose challenges in verifying data accuracy and combating disinformation. The role of Big Tech in elections was discussed, with stakeholders acknowledging its potential influence on electoral outcomes, even if direct evidence of this remains limited.

Therefore, there is an urgent need for the establishment of clear, structured guidelines and frameworks to ensure the effective use and management of electoral data. This includes promoting data transparency, strengthening access mechanisms and ensuring data integrity at every stage of the electoral process. Furthermore, stakeholders must be better equipped with tools and knowledge to navigate the evolving data landscape, leveraging technology to enhance the accuracy, accessibility and trustworthiness of electoral data. Only by addressing these gaps can the integrity of electoral processes be safeguarded, ensuring that elections are free, fair and credible.

7. Guidelines

Most interviewees indicated a lack of internal guidelines to direct the creation, use and availability of data internally, with some pointing to a paucity of such guidelines outside their organisations.

7.1 Elements of guidelines

The stakeholders suggested that elements included in the guidelines should be designed to support stakeholders in navigating the complex landscape of data management while upholding the core principles of open access, accuracy, trustworthiness and transparency. Stakeholders noted that guidelines should emphasise the non-negotiable integrity of data, encouraging practices that ensure information remains credible and reliable. Flexibility is paramount —guidelines must be adaptable rather than rigid to foster broader acceptance and application. The guidelines should focus on the quality and utility of data and information, steering clear of unnecessary complexities.

Recognising the bureaucratic hurdles that are often encountered when requesting data, these guidelines should offer practical insights for overcoming such challenges. They should provide strategies for accessing credible, publicly available information, especially free online data resources. Emphasis should be placed on the importance of ethical sourcing, timely access and the responsible transfer of data within established sharing agreements.

To ensure relevance in the evolving digital landscape, the guidelines incorporate international data protocols, promote Creative Commons licensing, and acknowledge the indispensable role of data holders' websites as key data sources. Additionally, in the context of AI, the guidelines adopt a less

prescriptive approach, recognising the dynamic nature of AI development and the need for adaptable governance frameworks. Based on stakeholders' input, elements of the guidelines must be aimed at creating a robust, flexible and ethical foundation for data stewardship, empowering users to engage with information responsibly and effectively.

7.2 Implementation advisory: access to data, elections and African standards

As noted earlier, the three sets of guidelines below for EMBs, political actors and civil society recognise that data (both public and private) is increasingly a key driver of processes and developments relevant to elections. Data informs decisions —whether automated by algorithms or made by humans—and is the fuel of machine-learning AI. Access to data should incorporate issues of privacy, storage, security, ethical use and sharing.

7.2.1 Implementation guidelines for EMBs on data access

Data, especially that used by social media, is increasingly a key driver of processes and outcomes relevant to elections. Data sets are used to inform decisions, including about electorally relevant information, and fuel machine-learning AI that can generate and direct content, and create fake identity profiles. See Appendix 4 for detailed guidelines for EMBs.

Therefore, the focus here is on how African EMBs can better understand the role of data in a national election so they can intervene as needed. It pinpoints actions needed for this, elaborates on what this entails, and provides legitimisation in a range of agreed pan-African and international standards.

Key action points and opportunities for EMBs

1. Reinforce the context:

- Support that the right to access public and relevant private information and data is legally guaranteed, and that requests are implemented and processed promptly and in accessible formats, and that there are reasons for refusals.
- Ensure that regulatory frameworks related to elections for digital platforms are effective, transparent and independently overseen, holding platforms accountable for: policy non-compliance; protecting freedom of expression; promoting media literacy; maintaining transparency in automated content moderation, supporting fact-checking; addressing harmful content; and ensuring accessible user reporting mechanisms.
- Ensure that digital platforms report on how they respect human rights by conducting due diligence addressing adverse impacts, implementing mitigations and taking steps to benefit election integrity, as well as adhering to international standards in platform design and content moderation. Ensure that platforms also report on their specific approaches concerning their roles in electoral risk assessment and related actions that benefit election integrity and mitigate harms.

2. Demand disclosure from social media:

- Promote platform transparency that provides accessible information including about efforts to fostering inclusivity, public participation and electoral integrity. Push companies to grant vetted researchers access to non-personal data and maintain transparency in political advertising.
- Require tech companies to disclose how they intend to use data to intervene in content moderation and advertising on their platforms. This should cover information about data harvesting, targeted advertising, and the sharing, ranking and/or removal of content, especially election-related content.

3. Form monitoring partnerships:

- Collaborate in order to understand disinformation campaigns during election processes to assess their impact on electoral integrity and public trust, while working to ensure compliance with privacy and data protection laws and also establishing mechanisms for the public to report concerns about online integrity issues.
- Create mechanisms with platforms and independent stakeholders to access data for monitoring social media and determine how platform mitigations are working during the election period. Support academic research on social media impacts and the safety of journalists and political candidates who are women.
- Use monitoring and reporting to ensure adherence to digital media guidelines by candidates and parties.

4. Communicate the results:

- Maintain an active, legally compliant and secure social media presence to prevent information gaps, while developing strategies to address misinformation and online threats throughout the election cycle.
- Proactively disclose key electoral information in an accessible, timely and affordable manner, ensuring the public's right to access is upheld, with clear processes for appeals and protections for whistleblowers disclosing wrongdoing in good faith.

5. Promote responsible use:

- Oversee the use of AI and data processing systems in line with international human rights standards.
- Ensure that the right to know in favour of election integrity includes legal guarantees for relevant public and private sector data sets, and that there are clear and justifiable reasons for refusals on disclosure.
- Require safeguards for data processing in content moderation and AI use to respect human rights.

6. Eliminate Gender Discrimination:

Work to eliminate discrimination against women through legal and practical measures, ensuring gender equality in constitutions and legislation and guaranteeing women's equal rights to vote, run for office, participate in policymaking, hold public positions and engage in political and civil society activities

7. Forge Collaboration:

Collaborate with journalists, media outlets, electoral practitioners and digital platforms to enhance transparency in content policies, ensure due process, establish independent oversight where necessary, and focus on providing accurate, diverse electoral information to the public while countering manipulation.

8. Promote Media and Information literacy:

Create opportunities for digital media and information literacy for all citizens especially for the youths and marginalised groups.

Nuts and bolts of action points

1. **Disclosure:** Social media companies should be asked for data and information about their risk analysis and planned mitigations for elections. It is important to know how they will use data for governing content and advertising, including how this could help promote the EMB's own content, and how content that is harmful to an election will be detected and demoted. This in turn can empower EMBs to negotiate with platforms to apply content moderation and curation measures. Data should be supplied on the numbers and linguistic competencies of their relevant teams, and on performance regarding threats and their mitigations, including response times. It is also important to have assurance that there are plans to protect personal data and prevent hack-attacks and other digital threats.
2. **Partnerships:** To verify claims made by social media companies and ensure oversight credibility, there must be a system that can independently monitor activities on the platforms. This means access to data at scale and analysis thereof. Because social media companies operating in most countries in Africa cannot be legally compelled to disclose data, voluntary partnerships must be sought to gain access to their Application Programme Interfaces through which bulk data can be obtained. Because most EMBs in Africa do not have their own data science capacity, partnerships are also needed to make meaningful sense of the monitoring—for example with reputable universities, civil society or specialised African companies.
3. **Communication:** Social media becomes a terrain of fierce electoral contestation. Therefore, EMBs as electoral umpires can build confidence in their oversight role by demonstrating to voters that they are on top of what is happening on the platforms and are in liaison with the private powers that control these platforms, to ensure a peaceful and positively informed electoral climate.

Underlying foundations

1. [Principles and Guidelines on the Use of Digital and Social Media](#)¹
2. [Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019](#)²
3. [Guidelines on Access to Information and Elections in Africa](#)³
4. [UN Guiding Principles on Business and Human Rights](#)⁴
5. [UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach](#)⁵
6. [“Journalism and Elections in Times of Disinformation” Addis Ababa Declaration on World Press Freedom Day 2019](#)⁶
7. [Malabo Convention](#)⁷
8. [The Convention on the Elimination of All Forms of Discrimination against Women \(CEDAW\)](#)⁸

7.2.2 Implementation guidance for political actors (parties, groups and independent candidates) on access to data in relation to elections

Purpose and use of this guideline

Data, especially data that is used by social media but also held by governmental bodies, is increasingly a key driver of processes and outcomes that are relevant to elections. Data sets serve to inform decisions, whether automated by algorithms or made by humans, and is also the fuel of machine-learning AI. It can also help understanding of technology-facilitated gender-based violence, particularly for women candidates, women members of political parties, political groups and independent candidates. This also includes women in polling centres and EMBS, and even women voters. See Appendix 5 for more details on implementation guidance for political actors.

Therefore, the focus here is on how political actors contesting African elections can better understand the value of data in a national poll, so they can act as needed. It pinpoints actions needed for this, elaborates on what this entails, and provides legitimization in a range of pan-African and international standards.

Key action points and opportunities

1. **Transparency:** Urge platform companies that their databases should increase transparency in political advert spending and targeting; urge governments to disclose election-relevant data on spending (for example, on public advertisements (ads), electoral subsidies and misuse of public infrastructure).

¹ <https://commspolicy.africa/wp-content/uploads/2023/11/AAEA-Guidelines.pdf>

² <https://achpr.au.int/en/node/902>

³ <https://achpr.au.int/en/node/894>

⁴ https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

⁵ <https://unesdoc.unesco.org/ark:/48223/pf0000387339>

⁶ https://au.int/sites/default/files/pressreleases/36586-pr-wpfaddisdecl3_may.pdf

⁷ <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

⁸ <https://www.un.org/womenwatch/daw/cedaw/cedaw.htm>

2. **Empowerment:** Multistakeholder efforts (by parties, platforms and others) to educate voters about data-driven campaigns on social media.
3. **Keep it clean:** Political parties must issue a public declaration refraining from use of digital disinformation and AI-fakes that are powered by data exploitation and give access to their own data on use of technology for content manipulation.

Nuts and bolts of action points

1. **Transparency:** Political advertising on social media can be covert through customised adverts seen only by certain audiences, and a lack of transparency about the variations, targeting, reach and spend. This means each party might be unaware of its rivals' online activity. Therefore, political parties should demand that social media companies create or improve repositories of political advertising, with the necessary detail for transparency. It is also important that voters can check such repositories where adverts should have identifiable provenance to enable them to identify fake party adverts. Regarding government spending, political parties have an interest in a fair playing field and monitoring potential bias by the authorities. This can be achieved through accessing data about election-related government spending.
2. **Empowerment:** Parties have an interest in voters being well informed about how data, algorithmic systems and co-ordinated campaigning can combine to boost social media virality. Voters should also be aware of data-driven microtargeting of content and advertising and be able to recognise when they are in a closed political bubble. This requires parties to disclose the content, origin and funding of online adverts, respecting data privacy through anonymisation and adhering to regulations on digital political advertising. Political contenders can encourage social media companies to reach every voter with messages and short courses that boost media and information literacy levels around the role of data for electoral integrity. They can also support media and information literacy programmes that empower users to critically engage with digital content, promote cultural diversity and gender equality, address the needs of vulnerable populations and collaborate with governments, digital platforms and stakeholders to reduce participation gaps and enhance digital literacy, especially during elections.
3. **Keep it clean:** Parties should boost their credibility as ethical players by publicly eschewing the use of digital manipulation techniques that exploit data in the information ecology of an election. This means not using deliberate lies and falsehoods in general, which create dirty data points, nor using patterns of data and data-driven systems to micro-target and spread such content. It also means parties should be transparent and provide access to campaign and spending data. Transparency is also needed for candidates who could be paying directly to the platforms, or for third-party actors paying candidates, parties or companies, for electoral campaigning.

Underlying foundations

1. [Principles and Guidelines on the Use of Digital and Social Media in Elections in Africa](#)

2. [Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019](#)
3. [Guidelines on Access to Information and Elections in Africa](#)
4. UN [Guiding Principles on Business and Human Rights](#)
5. UNESCO [Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach](#)

7.2.3 Implementation guidance for civil society on data access and elections

Purpose and use of this guideline

This guideline helps African civil society understand the role of data in national elections to enable informed interventions. It highlights key actions and their implications and aligns them with pan-African and international standards. See Appendix 6 for full implementation guide for civil society.

Key action points and opportunities for civil society

1. **Monitoring:** Increase capacity to collect and assess election-relevant data, including from social media, political parties and EMBs, including assessing data for media literacy, digital literacy and fact-checking initiatives.
2. **Collaboration:** Forge partnerships with EMBs and technology companies to monitor how platforms respond to challenges and promote opportunities for EMBs and oversight bodies to identify and mitigate digital and social media threats to the electoral process before they arise.
3. **Accountability:** Use data access to promote accountability by political parties, EMBs and platforms, including for election disputes, and educate voters about the role of data in elections and why transparency and data access is important. Advocate for Big Tech to ensure transparency in their election policies, content curation and moderation, including in local languages.

Nuts and bolts of action points

1. Civil society has an independent oversight role of social media activity and the response of platform companies during elections. Systematic monitoring is needed to detect content patterns (including adverts) that could violate human rights essential to election integrity. It is also needed to assess how companies respond to threats and promote opportunities for positive content. However, civil society needs a range of monitoring methods, such as donated access to data by companies, paid access (including via data broker firms), informal scraping and targeted probabilistic sampling, such as partnerships with groups subjected to harm (for example, women journalists). Ensuring privacy through anonymisation and disaggregated data is also important.
2. Without compromising independence, civil society actors can optimise their data access, build capacity and impact through structured relationships with EMBs and technology companies,

and work with academia to promote academic research on social media effects and the online safety of journalists and women in politics.

3. Advocate for strong legal frameworks, monitor data-related companies (especially during elections) and promote transparency and accountability in data practices to safeguard privacy and freedom of expression, in line with the UN Guiding Principles on Business and Human Rights. Advocate for individuals' rights and effective remedies for business-related human rights abuses, particularly around data access during elections, by supporting the establishment of judicial and non-judicial grievance mechanisms in line with Principles 25 and 27 of the UN Guiding Principles on Business and Human Rights. Raise awareness about data access rights and build capacity within communities to engage with businesses and governments on data-related issues. Civil society has a key role to raise awareness of data-driven challenges and opportunities during the election, as well as to publicise their own data-based evidence widely and incorporate all of this into capacity-building programmes for various stakeholders.

Underlying foundations

1. [Principles and Guidelines for the Use of Digital and Social Media in Elections in Africa](#)
2. [Declaration of Principles on Freedom of Expression and Access to Information in Africa](#)
3. [Guidelines on Access to Information and Elections in Africa](#)
4. UN [Guiding Principles on Business and Human Rights](#)
5. UNESCO [Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach](#)

References

African Alliance on Access to Data (AAAD). (2024). *Harnessing the Power of Data: A Commitment to Strengthening Access to Information in the Digital Age*.
<https://dataalliance.africa/unesco-iduai-2024-conference-statement-harnessing-the-power-of-data/>

Alvarez, R. M., & Hall, T. E. (2010). Electronic elections: The perils and promises of digital democracy. In *Electronic Elections: The Perils and Promises of Digital Democracy* (Vol. 9781400834082).

Association of African Election Authorities. (2024). *PRINCIPLES AND GUIDELINES FOR THE USE OF DIGITAL AND SOCIAL MEDIA IN ELECTIONS IN AFRICA*.
<https://www.elections.org.za/content/Documents/Event-materials/2024-Principles-and-Guidelines-for-the-Use-of-the-Digital-and-Social-Media-in-Elections-in-Africa/English---Principles-and-Guidelines-for-the-Use-of-the-Digital-and-Social-Media-in-Elections-in-Africa/>

Borgesius, F. J. Z., Möller, J., Kruikemeier, S., Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, 14(1). <https://doi.org/10.18352/ulr.420>

CIPESA. (2024). *2024 State of Internet Freedom in Africa Report Unveils the Promises and Challenges of Technology in African Elections*.
<https://cipesa.org/2024/09/2024-state-of-internet-freedom-in-africa-report-unveils-the-promises-and-challenges-of-technology-in-african-elections/>

Dunning, T., Grossman, G., Humphreys, M., Hyde, S. D., McIntosh, C., & Nellis, G. (2019). Do Informational Campaigns Promote Electoral Accountability? In *Information, Accountability, and Cumulative Learning: Lessons from Metaketa I*.
<https://doi.org/10.1017/9781108381390.002>

Gadasu, E. K. (2024). *Data Protection and Privacy in Elections: The Ghanaian Context*.
<https://iipgh.org/data-protection-and-privacy-in-elections-the-ghanaian-context/>

Itodo, S. (2024). *Artificial Intelligence and the integrity of African elections*. International IDEA.
<https://Www.Idea.Int/News/Artificial-Intelligence-and-Integrity-African-Elections>.

Birch, S. (2013). Electoral Malpractice - By Sarah Birch. *Political Studies Review*, 11(1).
<https://global.oup.com/academic/product/electoral-malpractice-9780199606160?cc=ca&lang=en&#>

Norris, P. (2014). Why electoral integrity matters. In *Why Electoral Integrity Matters* (Vol. 9781107052802). <https://doi.org/10.1017/CBO9781107280861>

Open Elections Data Initiative. (2024). *Open Election Data Principles*.
<https://openelectiondata.net/en/guide/principles/>

IDEA. (2022). The Global State of Democracy 2022: Forging Social Contracts in a Time of Discontent. In *The Global State of Democracy 2022: Forging Social Contracts in a Time of Discontent*. <https://doi.org/10.31752/idea.2022.56>

IDEA. (2023). The Global State of Democracy 2023: The New Checks and Balances. In *The Global State of Democracy 2023: The New Checks and Balances*. <https://doi.org/10.31752/idea.2023.78>

Appendices

Appendix 1

Proposed publicity programme

The following opportunities can be used to promote guidelines on election data integrity to civil society, media, political parties and EMBS:

1. **Leverage regional and pan-African electoral events** such as the AU's Annual Dialogue on Democracy, Governance and Human Rights Symposium, and the Economic Community of West African States (ECOWAS) Network of Electoral Commissions meetings by organising side events, workshops or panel discussions.
2. **Create partnerships with international organisations**, such as collaborations with bodies including the UN Economic Commission for Africa (UNECA), the UN Development Programme (UNDP), International IDEA and the Carter Center through joint events or joint reports highlighting the guidelines' relevance.
3. **Integrate into election observation missions** by taking advantage of opportunities to work with AU Election Observation Missions (AUEOM), East African Community (EAC) Election Observation Missions, ECOWAS Election Observation Missions, and the Southern African Development Community (SADC) Electoral Advisory Council (SEAC) to incorporate guidelines into their activities.
4. **Engage with digital and technology conferences in Africa** by presenting at relevant events such as Africa Tech Summit, RightsCon, Smart Africa, and the Africa Internet Governance Forum (AfIGF).
5. **Hold national-level workshops with EMBs and political parties** during the election cycle that target EMBs, political parties and civil society organisations.
6. **Launch media engagement and public awareness campaigns** using traditional and digital media platforms, including op-eds, radio discussions and infographics in local languages to highlight key aspects of the guideline for a wider reach.
7. **Integrate academic partnerships for research and curriculum** by partnering with African universities, think tanks and research centres specialising in political science, governance and data studies to encourage policy research projects, student debates and curriculum modules based on the guidelines.
8. **Collaborate with social media platforms** such as Meta (Facebook), X (formerly Twitter), TikTok and Google on election integrity programmes by advocating for platform-specific policy changes that reflect the guidelines' recommendations.
9. **Use election-related international days**, such as International Day of Democracy (September 15) and Global Elections Day (the first Thursday of February), to stage public dialogues, online campaigns and expert panels.
10. **Leverage regional networks and coalitions of civil society organisations** such as the African Democracy Forum (ADF), CIVICUS, Pan African Parliament Civil Society Forum, Association for Progressive Communications (APC) and the West African Civil Society Forum (WACSO) by training trainers within these networks to cascade guideline knowledge across communities.

Appendix 2 – List of interviewees

1. Brett Horner, Editor, AFP Fact Check, South Africa
2. Nathan Gadugah, Editor, Dubawa, Ghana
3. Noko Makgato, Executive Director, Africa Check, South Africa
4. David Oluwamayowa Ajikobi, Editor, Africa Check, Nigeria
5. Demba Kandeh, Editor, FactSpace West Africa, The Gambia
6. Mariama Thiam, Country Director, Centre for Journalism Innovation & Development (CJID), Senegal
7. Dr Aurelia Ayisi, Lecturer, University of Ghana, Department of Communication Studies, Ghana
8. Two Senior Officers from different EMBS
9. Senior Officer from a Pan-African civil society organisation
10. Olufunto Akinduro, Senior Programme Officer, Africa and West Asia, IDEA
11. Hon Stanley Olajide Adedeji, Member of the Federal House of Representatives, Representing Ibadan North West/South West Constituency, Nigeria
12. Mariam Jobe, Ministry of Communications and Digital Economy, The Gambia
13. Fola Oduduwa, Senior Associate, RIA, Nigeria
14. Shuaib Afolabi Salisu, Nigerian Senator for Ogun Central constituency of Ogun State
15. Mabinty Alice Taylor-Bangura, Member of Parliament, Northwest Region, Sierra Leone

Appendix 3 – Research instrument

Action research: Guidelines on access to data for key stakeholders in African elections

Research ICT Africa (RIA) <https://researchictafrica.net> in association with the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) <https://cipesa.org>

Researcher: Kwami Ahiabenu PhD

QUESTIONS

(Questions to be modified for each stakeholder group)

Interviewees

1. Election management bodies (EMBs)
2. Political parties

3. Media
4. Civil society
5. Researchers, fact-checkers and academics
6. Others

Sought verbal informed consent and permission to record

Section A: General information

1. Name of respondent:
2. Organisation:
3. Country:
4. Role within organisation and experience in election-related activities:

Section B: Data usage in elections

1. In what ways does your organisation use data throughout the electoral cycle?
2. What specific types of elections data are most valuable to your organisation? (Probe voter registration data, election results, opinion poll, campaign financing data, polling station data, campaign data, social media, government data, etc.).
3. How do you access data for election-related activities?
4. Can you describe any challenges you have faced in accessing the necessary election data? (Probe data availability, data accuracy, timeliness of data, data security and privacy concerns, and inability to secure data from Big Tech or official sources).

Section C: Enabling environment for electoral data access

1. What are the current laws in your country regarding freedom of information, and how do they affect your organisation's access to public and private data?
2. Does your country have policies that promote or restrict access to election-related data? (Probe open elections data initiatives and open government partnerships).
3. How does the Freedom of Information law in your country enable or limit your access to critical election data?

Section D: Big Tech and access to electoral data

1. In your experience, how have major tech companies (e.g., Google, Facebook, Twitter) facilitated access to election-related data for your organisation?

2. Do you believe that partnerships with Big Tech companies are possible, and if so, can they improve access to real-time election data?
3. Have you encountered challenges when attempting to access election-related data from Big Tech platforms?
4. Do you think the algorithms and policies of Big Tech companies restrict or manipulate the flow of election-related information?
5. How well do Big Tech companies balance transparency with security and privacy concerns when sharing election-related data?
6. In what ways do you believe Big Tech can influence the outcome or integrity of elections through their data management practices?

Section E: Guidelines for data access

1. Does your organisation follow any formal guidelines for accessing and using election data?
2. How important is it for your organisation to have standardised guidelines on data access for election integrity?
3. What specific elements should be included in data access guidelines to improve election integrity? (Probe data security protocols, data sharing agreements, ethical data use policies, public transparency of data, timeliness and availability of data).
4. Can you share any example of guidelines on access to elections data?
5. How can we tailor electoral data access guidelines to fit different cultural and contextual factors?

Section F: Improving election integrity

1. Can you give examples of how better data access could enhance the integrity of elections?
2. How do you ensure that the data your organisation uses is accurate and reliable?
3. In your opinion, how can better access to election data improve election integrity? (Probe increased transparency, better voter engagement, enhanced fraud detection, improved electoral management).
4. Does your organisation have opportunities to undertake training on how to use election data more effectively?
5. Would your organisation benefit from training on how to use election data more effectively?
6. In your opinion, how would you improve transparency, security or accuracy of data that impacts election outcomes?

Conclusion

Please share any additional comments, suggestions or recommendations on how data access can be improved to support election integrity.

Appendix 4 Guiding clauses for action points on data access for EMBs

Recap of action points for EMBs

1. **Disclosure:** Social media companies should be asked for data and information about their risk analysis and planned mitigations for elections. It is important to know how they will use data for governing content and advertising, including how this could help promote the EMB's own content, and how content that is harmful to an election will be detected and demoted. This in turn can empower EMBs to negotiate with platforms to apply content moderation and curation measures. Data should be supplied on the numbers and linguistic competencies of their relevant teams, and on performance regarding threats and their mitigations, including response times. It is also important to have assurance that there are plans to protect personal data and prevent hack-attacks and other digital threats.
2. **Partnerships:** To verify claims made by social media companies and ensure oversight credibility, there must be a system that can independently monitor activities on the platforms. This means access to data at scale and analysis thereof. Because social media companies operating in most countries in Africa cannot be legally compelled to disclose data, voluntary partnerships must be sought to gain access to their Application Programme Interfaces through which bulk data can be obtained. Because most EMBs in Africa do not have their own data science capacity, partnerships are also needed to make meaningful sense of the monitoring —for example, with reputable universities, civil society or specialised African companies.
3. **Communication:** Social media becomes a terrain of fierce electoral contestation. Therefore, EMBs as electoral umpires can build confidence in their oversight role by demonstrating to voters that they are on top of what is happening on the platforms and are in liaison with the private powers that control these platforms, to ensure a peaceful and positively informed electoral climate.

Underlying foundations:

1. Principles and Guidelines on the Use of Digital and social media⁹
2. Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019¹⁰
3. Guidelines on Access to Information and Elections in Africa¹¹
4. UN Guiding Principles on Business and Human Rights¹²
5. UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach¹³

⁹ <https://commspolicy.africa/wp-content/uploads/2023/11/AAEA-Guidelines.pdf>

¹⁰ <https://achpr.au.int/en/node/902>

¹¹ <https://achpr.au.int/en/node/894>

¹² https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

¹³ <https://unesdoc.unesco.org/ark:/48223/pf0000387339>

6. “[Journalism and Elections in Times of Disinformation](#)¹⁴” *Addis Ababa Declaration on World Press Freedom Day, 2019*
7. Malabo Convention¹⁵
8. The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)¹⁶

Relevant clauses from foundational documents for each EMB action point.

	Instrument	Clause/s
Action 1: Demand disclosure from social media companies	AAEA Principles and Guidelines	The clauses emphasise compliance with privacy and data protection laws throughout the electoral cycle, following international standards (Clause 9.6). Digital and social media platforms must have mechanisms for reporting election-related integrity issues (Clause 9.7) and conducting human rights due diligence (Clause 11.1). They should provide clear, accessible information (Clause 11.4) and ensure transparency in election policies, content moderation, and multilingual capacities (Clause 11.5). Recommender systems must not process sensitive personal data (Clause 11.13). AI interactions should be transparent (Clause 11.16), and data protection authorities should uphold privacy rights in elections (Clause 12.5).
	Malabo Convention	The relevant provisions are Article 2.2, Scope of application, Article 13, Principle 5 - Transparency of data processing, Article 16, Right to Information and Article 17, Right of Access
	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	The right of access to information must be legally guaranteed, allowing individuals to access public and relevant private information quickly and affordably (Principle 26). This right follows the principle of maximum disclosure, with only narrowly defined exemptions (Principle 28). Public and private bodies must maintain information to facilitate access (Principle 30), and requests should be processed promptly, in accessible formats, without requiring justification

¹⁴ https://au.int/sites/default/files/pressreleases/36586-pr-wpfdaddisdecl3_may.pdf

¹⁵ <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

¹⁶ <https://www.un.org/womenwatch/daw/cedaw/cedaw.htm>

		(Principle 31). Refusals must be well-reasoned and subject to free internal and legal appeals (Principle 32). Exemptions apply only when harm outweighs public interest (Principle 33), and violations of disclosure obligations are punishable by law (Principle 36). Internet intermediaries must ensure human rights safeguards in content moderation, transparency in content removal, and AI use aligned with international human rights standards (Principle 39).
	ACHPR Guidelines on Access to Information and Elections in Africa, 2017	The Guidelines provide direction to electoral stakeholders on the proactive disclosure of information to ensure electoral integrity and public trust. They apply to election authorities, political parties, law enforcement, media, civil society, and other key actors. Access to information is a fundamental right, with a duty to disclose unless narrowly justified exemptions apply. Electoral stakeholders must create, maintain, and publish key electoral information in an accessible manner. The process for accessing information must be simple, quick and affordable, with refusals subject to appeal. Whistleblowers who disclose wrongdoing in good faith are protected from sanctions.
	The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies (A/HRC/50/56) https://www.ohchr.org/en/publications/referen ce-publications/guiding-principles-business-and-human-rights	Focusing on Corporate responsibility to respect human rights (pillar II): Businesses must respect human rights by avoiding and addressing adverse impacts linked to their operations. This responsibility applies universally and aligns with international human rights standards. Companies should implement policies, conduct human rights due diligence, and establish remediation processes. They must integrate human rights considerations into operations, monitor their impact, and communicate their efforts transparently. When harm occurs, businesses should provide or support remediation. In all contexts, they must comply with laws, uphold international human rights, and prioritise addressing severe risks.

	UN Guiding Principles on Business and Human Rights	EMBs may reference this provision of the Guiding Principles on Business and Human Rights when engaging with social media companies. It states that businesses should communicate externally about their human rights impact, especially when concerns are raised by affected stakeholders. Those operating in high-risk contexts must formally report on how they address such impacts.
	UNESCO Guidelines for the Governance of Digital Platforms	Digital platforms have a responsibility to respect human rights by adhering to five key principles: conducting human rights due diligence, following international human rights standards in platform design and content moderation, ensuring transparency, providing accessible information, and being accountable to stakeholders. They must apply these principles in all jurisdictions where they operate. Governance systems should emphasise transparency, inclusivity, and public participation. Platforms should also grant vetted researchers access to non-personal data while safeguarding privacy. For electoral integrity, platforms must assess risks, engage with stakeholders, ensure access to diverse viewpoints, and maintain transparency in political advertising.
	Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)	States must eliminate discrimination against women through legal and practical measures, ensuring gender equality in constitutions and legislation. They must prohibit discrimination by individuals, organisations, and businesses. Women must have equal rights to vote, run for office, participate in policymaking, hold public positions, and engage in political and civil society activities.

	Addis Ababa Declaration	Journalists, media outlets, electoral practitioners, and digital platforms should enhance transparency in content policies, ensure due process, and establish independent oversight where necessary. UNESCO Member States and Electoral Management Bodies should implement Right to Information laws per Sustainable Development Goal (SDG) 16.10. Efforts should focus on providing accurate, diverse electoral information to the public and countering manipulation. Additionally, guidelines for AI use in media should be developed to safeguard freedom of expression and human rights.
Action 2: Monitoring partnerships	AAEA Principles and Guidelines	EMBs should enhance their digital and social media expertise, collaborate with researchers, and establish transparent agreements with digital platforms to protect user rights. They must monitor online activity throughout the electoral cycle, ensuring candidates and parties adhere to digital media guidelines. EMBs should oversee political advertising transparency and work with various stakeholders to detect and mitigate digital threats to elections. Social media platforms should facilitate vetted data access for research on electoral integrity.
	UNESCO Guidelines for the Governance of Digital Platforms	Regulatory frameworks for digital platforms should be effective, transparent and independently overseen. Platforms must be held accountable for policy non-compliance and protecting freedom of expression, with proportionate enforcement measures. Self-regulation should include independent audits, while co-regulation involves collaboration between industry and public authorities. Statutory regulation should focus on systems and processes rather than individual content legality. Platforms should promote media literacy, establish accessible user reporting mechanisms, and ensure culturally sensitive complaint handling. For electoral integrity, they should address harmful content, support fact-checking, and maintain

		transparency in automated content moderation tools.
	Addis Ababa Declaration	<p>Carry out independent analysis of disinformation campaigns during election processes and their impact on elections.</p> <p>Call on journalists, media outlets, electoral practitioners, Internet intermediaries and social media practitioners to consider exposing disinformation and propaganda, particularly during elections, in fulfilment of a journalistic watchdog role in society and the news media's mandate to contribute to debates on matters of public interest.</p>
Action 3: Communicate	AAEA Principles and Guidelines	EMBs should maintain an active, legally compliant and secure social media presence to prevent information gaps (Clause 10.2.2). They should also develop strategies to address misinformation and online threats, safeguarding the integrity of elections throughout the election cycle (Clause 10.14).
	ACHPR Guidelines on Access to Information and Elections in Africa, 2017	Implementation 34: State Parties shall, in each Periodic Report submitted to the African Commission in accordance with Article 62 of the African Charter, provide detailed information on the measures taken to facilitate compliance with the provisions of these Guidelines.
	UNESCO Guidelines for the Governance of Digital Platforms	Digital platforms should ensure transparency through regular public reporting on their adherence to transparency principles, responses to government requests, and performance against their terms of service (Principle 3). This includes providing clear, accessible information in users' languages, with effective content moderation and complaint processes. For electoral integrity, platforms should engage with stakeholders, clearly label political ads with funding details, and monitor the monetisation of political content.
	Addis Ababa Declaration	Promote Media and Information Literacy, especially

		among youth, through formal, informal and non-formal education. Support academic research on social media impacts and journalist safety to inform evidence-based institutional responses. Uphold the public's Right to Information, expand media literacy, and ensure journalist safety—particularly for women—as critical measures to address electoral challenges.
--	--	--

Appendix 5 Guiding clauses for action points on data access for political actors (parties, groups and independent candidates)

Recap of action points for political actors

1. **Transparency:** Political advertising on social media can be covert through customised adverts seen only by certain audiences, and a lack of transparency about the variations, targeting, reach and spend. This means each party might be unaware of its rivals' online activity. Therefore, political parties should demand that social media companies create or improve repositories of political advertising, with the necessary detail for transparency. It is also important that voters can check such repositories where adverts should have identifiable provenance to enable them to identify fake party adverts. Regarding government spending, political parties have an interest in a fair playing field and monitoring potential bias by the authorities. This can be achieved through accessing data about election-related government spending.
2. **Empowerment:** Parties have an interest in voters being well informed about how data, algorithmic systems and co-ordinated campaigning can combine to boost social media virality. Voters should also be aware of data-driven microtargeting of content and advertising and be able to recognise when they are in a closed political bubble. Social media companies can reach every voter with messages and short courses that boost media and information literacy levels around the role of data for electoral integrity.
3. **Keep it clean:** Parties should boost their credibility as ethical players by publicly eschewing the use of digital manipulation techniques that contaminate data in the information ecology of an election. This means not using deliberate lies and falsehoods in general, which create dirty data points or exploit patterns of data and data-driven systems to target and spread such content. It also means parties should be transparent and provide access to campaign and spending data. Transparency is also needed for candidates who could be paying directly to the platforms or for third-party actors paying candidates, parties or the companies for electoral campaigning.

Underlying foundations

1. [Principles and Guidelines on the Use of Digital and Social Media in Elections in Africa](#)
2. [Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019](#)
3. [Guidelines on Access to Information and Elections in Africa](#)
4. UN [Guiding Principles on Business and Human Rights](#)
5. UNESCO [Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach](#)

Relevant clauses from the foundational documents for each political party action point.

Action	Instrument	Clause/s
Action 1: Transparency	AAEA Principles and Guidelines	Microtargeting is an online advertising technique that analyses personal data to deliver personalised messages to specific individuals or audiences, often via social media. Social media platforms should provide clear, accessible information throughout the electoral cycle about political ads, including their content, origin, funding, and a repository of such ads. Individuals may consent to their data being used for advertising, but this data must be anonymised before sharing with third parties. Regulatory bodies are encouraged to establish rules governing political microtargeting and online political advertising, outlining the responsibilities of candidates, parties and digital platforms.
	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	Principle 41 emphasises the protection of privacy in communication surveillance. States must not engage in indiscriminate data collection, storage, analysis or sharing. Any law permitting targeted surveillance must include safeguards such as independent judicial authorisation, due process, clear limitations on scope and duration, timely notification after

		surveillance concludes, transparency about surveillance practices, and oversight by an independent review body.
	ACHPR Guidelines on Access to Information and Elections in Africa, 2017	25. Media and internet regulatory bodies shall adopt regulations on media coverage during elections that ensure fair and balanced coverage of the electoral process and transparency about political advertising policy on media and online media platforms.
	UNESCO Guidelines for the Governance of Digital Platforms	<p>Principle 3: Platform Transparency</p> <p>Digital platforms should regularly report on their adherence to transparency principles, including responses to government content requests, with adjustments based on company size to ease burdens on smaller entities. Transparency must be clear, concise and meaningful, providing stakeholders with actionable information beyond legal texts or data dumps.</p> <p>Platforms must publicly disclose:</p> <ul style="list-style-type: none"> • Content Moderation & Terms of Service: Measures for moderating content, enforcement processes, reasons for content restrictions, and policies on user account suspensions. • Moderation Practices: Use of automated tools, human oversight, policy changes, and safeguards for freedom of

		<p>expression, including moderator expertise and roles.</p> <ul style="list-style-type: none"> • Data Handling: How personal data is collected, used and shared, especially regarding algorithmic decision-making. • User Complaints: Processes for appeals, outcomes of complaints, and responses to state officials' requests. • Advertising Transparency: Details on political ads, data-driven targeting practices, human rights impact assessments, and machine-generated content labeling. <p>Independent evaluations of transparency measures should be conducted regularly, with findings made publicly available.</p>
	Addis Ababa Declaration	<p>Call on journalists, media outlets, electoral practitioners, internet intermediaries and social media practitioners to consider mechanisms to ensure that digital advertising, including political advertising, makes the source clear, and avoids the misrepresentation of identities and invisible funding.</p>
Action 2: Empowerment	AAEA Principles and Guidelines	<p>Media and Information Literacy, and Digital Literacy</p> <p>Media and information literacy involves the knowledge, attitudes and skills needed to engage critically with media content and technologies, while digital literacy focuses on competencies for using digital tools. Both are vital for elections.</p>

		<p>Electoral stakeholders should:</p> <ul style="list-style-type: none"> • Ensure marginalised and vulnerable groups have equal access to digital platforms, online safety and literacy programs. • Partner with stakeholders to empower youth as informed digital media creators and consumers, integrating voter education. • Encourage social media operators to promote voter registration, share reliable electoral information, and support media and digital literacy initiatives, especially for marginalised groups.
	<p>Other instruments</p>	<p>Media and Information Literacy (MIL)</p> <p>Media and Information Literacy (MIL) encompasses critical thinking skills that enable users to engage effectively with digital content. Its promotion requires collaboration among governments, digital platforms and stakeholders to share knowledge, resources and a unified vision.</p> <p>MIL programmes should:</p> <ul style="list-style-type: none"> • Empower users with skills to critically analyse diverse media content, beyond just digital safety, following best practices from UNESCO and other bodies. • Promote cultural diversity, social inclusion, gender equality and

		<p>global citizenship, while reducing participation gaps for marginalised groups.</p> <ul style="list-style-type: none"> Address the needs of vulnerable populations, including women, girls and children through targeted education and awareness campaigns on digital rights and safety. <p>Governments and digital platforms should:</p> <ul style="list-style-type: none"> Develop public strategies to enhance MIL and digital literacy, with dedicated resources and training for both users and product development teams. Implement monitoring mechanisms to evaluate MIL initiatives and collaborate with independent experts, civil society, educators and cultural professionals. Foster user awareness of their online and offline rights, particularly regarding freedom of expression and access to information.
Action 3: Keeping it clean	AAEA Principles and Guidelines	<p>Data Protection and Ethical Conduct in Elections</p> <p>All stakeholders in the electoral process must comply with privacy and personal data protection laws, guided by international standards such as purpose limitation, fairness, transparency, data minimisation, storage limitation, accuracy,</p>

		<p>confidentiality, integrity and accountability.</p> <p>Political parties and candidates are expected to:</p> <ul style="list-style-type: none"> • Avoid supporting or condoning any form of online harm, including actions by their supporters, throughout the electoral cycle. • Ensure transparency in digital and social media campaigns, with clear attribution for paid content, including influencer marketing. • Uphold data protection principles and safeguard voters' fundamental rights, particularly concerning personal data.
	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	<p>Principle 23: Prohibited speech</p> <p>1. States shall prohibit any speech that advocates for national, racial, religious or other forms of discriminatory hatred which constitutes incitement to discrimination, hostility or violence.</p>
	Addis Ababa declaration	<p>Call on each UNESCO Member State, including their Electoral Management Bodies, to avoid making, sponsoring, encouraging or further disseminating statements which they know (or reasonably should know) to be false (disinformation), or which demonstrate a reckless disregard for verifiable information (propaganda), as well as statements that undermine the credibility of journalists and media or label them as enemies, liars or opposition.</p>

		<p>Promote a code of conduct among political actors to avoid the use of disinformation campaigns in electoral processes and the establishment of accountability mechanisms related to the violation of such a code.</p>
	<p>The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies (A/HRC/50/56)</p>	<p>Transparency of Political Advertising on Digital Platforms</p> <p>Digital platforms involved in electoral advertising must:</p> <ul style="list-style-type: none"> • Clearly label political ads and outline responsibilities in their terms of service regarding transparency on funding sources, amounts, and sponsors. • Track the monetisation of posts by political parties and their representatives. • Publicly disclose demographic targeting details of political ads. • Maintain a publicly accessible, regularly updated online library containing these ads and related funding information.

Appendix 6 Guiding clauses for action points on data access for civil society

Recap of action points for civil society

1. Civil society has an independent oversight role during elections, monitoring social media activity and the response of platform companies. Systematic monitoring is needed to detect content patterns (including ads) that could violate human rights essential to election integrity. It is also needed to assess how companies respond to threats and promote opportunities for positive content. However, civil society needs a range of monitoring methods, such as donated access to data by platform companies, paid access (including via data broker firms), informal scraping and targeted probabilistic sampling, such as partnerships with groups subjected to harm (for example, women journalists).

2. Without compromising independence, civil society actors can optimise their data access, capacities and impact through structured relationships with EMBs and technology companies.
3. Civil society has a key role to raise awareness of data-driven challenges and opportunities during the election, to publicise their own data-based evidence widely and to incorporate all of this into capacity-building programmes for various stakeholders.

Underlying foundations

1. [Principles and Guidelines for the Use of Digital and Social Media in Elections in Africa](#)
2. [Declaration of Principles on Freedom of Expression and Access to Information in Africa](#)
3. [Guidelines on Access to Information and Elections in Africa](#)
4. UN [Guiding Principles on Business and Human Rights](#)
5. UNESCO [Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach](#)

Relevant clauses from the foundational documents for each civil society action points.

	Instrument	Clause/s
Action 1: Monitor	AAEA Principles and Guidelines	Social media operators should ensure transparency and accountability in their election policies, content curation and moderation, including in local languages. They should collaborate with key stakeholders to publicise standards and reporting mechanisms for harmful election content and provide vetted data access for electoral integrity research.
Action 2: Collaborate	AAEA Principles and Guidelines	EMBs and oversight bodies should collaborate with key stakeholders to identify and mitigate digital and social media threats to the electoral process before they arise.
Action 3: Empower	AAEA Principles and Guidelines	Civil society organisations should collaborate with key stakeholders to promote media literacy, digital literacy, and fact-checking initiatives.
	Addis Ababa Declaration	Promote academic research specialising in the impact of social media and journalistic safety to

		ensure evidence-based institutional and state responses.
Action: Research	UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach	<p>The Role of Civil Society, Transparency and Data Access on Digital Platforms</p> <ul style="list-style-type: none"> • Research and Data Access: Researchers should have access to disaggregated, non-personal, and pseudonymous data to analyse the impact of digital platforms on various groups, considering gender, race, age and other intersecting factors. Platforms should facilitate this through APIs and reliable data interfaces. • Transparency: Digital platforms must provide clear, detailed and meaningful information about their automated systems, data collection, targeted advertising and content moderation practices, particularly concerning election-related content. • Advertising Practices: Platforms should disclose details on targeted demographics, funding sources and human rights impacts of advertising systems. They must maintain a publicly accessible, regularly updated online library of political ads. • Protections for Vulnerable Groups: Special protections should be in place for women, marginalised groups, and defenders of human rights. Privacy-protecting technologies should support external research on algorithmic amplification of online violence.
Action: Advocacy	UNESCO Guidelines for the governance of digital platforms: safeguarding	Data Access and Electoral Integrity on Digital Platforms

	<p>freedom of expression and access to information through a multi-stakeholder approach</p>	<ul style="list-style-type: none"> ● Data Access: Digital platforms should provide non-personal data to journalists and advocacy groups when it's in the public interest, ensuring privacy through measures like anonymisation and safeguarding commercial confidentiality. Reliable data interfaces should offer disaggregated data based on factors like gender, race and age, guided by governance systems on proportionality and relevance. ● Electoral Integrity: Platforms must ensure users can access diverse election-related content without undue restriction from automated tools, in line with international human rights standards.
<p>Action: Empower</p>	<p>UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach</p>	<p>26. Specifically, states should:</p> <p>c) Direct resources and accelerate efforts to close the digital divide, fill data gaps, remove other barriers faced by groups in situations of vulnerability and marginalisation, and fulfil all women's and girls' right to access to information.</p>
<p>Action: Collaborate</p>	<p>UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach</p>	<p>50. Governance systems should also promote dialogue with media, including for the investment in independent news media, and support the media ecosystem by making data available and supporting actions to bolster media sustainability, diversity and plurality.</p>

Action: Due diligence	UNGPs on business and human rights	<p>Human Rights Due Diligence and the Role of Civil Society</p> <ul style="list-style-type: none"> ● Business Responsibility: Under the UN Guiding Principles (UNGPs), businesses must conduct human rights due diligence, including assessing, addressing, tracking, and communicating actual or potential human rights impacts arising from their activities or business relationships. ● State and Civil Society Roles: States are responsible for protecting human rights by regulating businesses within their jurisdiction. Civil society organisations can advocate for strong legal frameworks, monitor data-related companies (especially during elections), and promote transparency and accountability in data practices to safeguard privacy and freedom of expression.
Action: Access to remedy	UNGPs on business and human rights	<p>Principle 25 emphasises that States have a responsibility to ensure access to effective remedies for individuals affected by business-related human rights abuses within their territory. Principle 27 underscores the importance of establishing both judicial and non-judicial grievance mechanisms as part of a comprehensive system for addressing these abuses. Civil society organisations can significantly contribute by advocating for individuals' rights and seeking remedies, particularly concerning human rights violations related to data access during elections.</p>

Action: Awareness and capacity building	UNGPs on business and human rights	<p>Principle 3: Under operational principles</p> <p>*Civil society organisations can raise awareness about the UNGPs among their constituencies, empowering individuals to understand their rights regarding data access. Additionally, they can build capacity within their communities to engage with businesses and governments on data-related issues.</p>
Action: Multi-stakeholder engagement	UNGPs on business and human rights	<p>Principle 3: Under operational principles</p> <p>*Civil society organisations can facilitate dialogue and partnerships between civil society, businesses, and governments to collaboratively address challenges related to data access. This could involve participating in multi-stakeholder initiatives, consultations, or forums to influence policies and practices.</p>
Action: Documentation and advocacy	UNGPs on business and human rights	<p>Principle 3: Under operational principles</p> <p>Civil society can document and highlight instances where data practices impact human rights negatively. Through research, advocacy, and campaigns, civil society organisations can draw attention to potential abuses and press for corrective actions.</p>