Guideline for election stakeholders and ATD

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

This document comprises useful guides for three constituencies. The first guide is for EMBs; the second for political actors especially political parties; the third for civil society.

 [For the future: other toolkits can be developed with different stakeholder groups covering different issues: eg. access to information groups and data access; media (and media viability) and data access; climate change and data access; content regulators (eg. AV regulators); AI start-ups etc; Info commissioners and data access; security cluster and data access; sexual and reproductive rights, and data access, lawyers and data access; civic tech and data access; parliamentarians and data access; judicial actors and data access; etc.)

This particular guide is based on the recognition that data (both public and private) is increasingly a key driver of processes and developments that are relevant to elections. Data informs decisions - whether automated by algorithms, or made by humans, and data is the fuel of machine-learning AI. Access to data should incorporate issues of privacy, storage, security, ethical use, and sharing.

Therefore the focus below is on how actors (specifically African EMBs, political parties and civil society) can get a greater understanding of the role of data in a national election. It pinpoints the actions needed to achieve this, elaborates on what these actions entail, and provides the reference point in a range of agreed pan-African and international standards. The three-part package can help stakeholders implement their mandate/mission in digital times, in alignment with these standards.

=

Specs:

2 or 3 page length of core guide, per stakeholder group (EMBs, political parties, civil society), *plus* Appendix in each case *with details on relevant African standards*. To output in English and French.

Actions by the coalition: to convene targeted webinars in partnership with stakeholder groups (eg. AAEA, IDEA, EISA), then to update/revise and finally seek a form of direct or indirect recognition from the ACHPR .

Timing: Feb – presentation to the AAEA meeting of about 22-25 African EMBs in Johannesburg 27/29 Feb; 20 TAEF agenda, African Media Festival 21-22?, March – April: webinars; May revisions; Subsequently: discussions with ACHPR and other AU partners.

==

A. Implementation guidelines for EMBs on data access

Purpose and use of this guideline

Data, especially that used by social media, is increasingly a key driver of processes and outcomes that are relevant to elections. Data sets are used to inform decisions, including about electorally-relevant information - whether automated by algorithms, or made by humans, and data is also the fuel of machine-learning AI that can generate content, target it, and create fake identity profiles .

Therefore the focus here is on how African EMBs can get a greater understanding of the role of data in a national election, so they can intervene as needed. It pinpoints the actions needed for this,

elaborates on what these entail, and provides the legitimation in a range of agreed pan-African and international standards.

Key action points/opportunities for EMBs:

1. **Demand disclosure from social media**: Require tech companies to disclose their specific approaches concerning their roles in electoral risk assessment and related actions benefiting election integrity and mitigating harms, and how they intend to use data to intervene in both content 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

2. **Make partnerships to monitor**: Create mechanisms with platforms and independent stakeholders to access data for monitoring of what's happening on social media (and how platform mitigations are working), during the election period.

3. **Communicate the results**: Publicise any data-related findings from the first two actionables.

What's entailed in each Action point:

1. **Disclosure**: In line with transparency, social media companies should be asked for data and information about their risk analysis and planned mitigations for the elections. It is important to know how they will be using data for governing content and advertising, in regard to how, for example, this could help promote the EMB's own content, and detecting and demoting content for which an assessment shows that it can clearly harm the election. This in turn can empower EMBs to negotiate with platforms to apply content moderation and curation measures. Data should be supplied on their numbers and linguistic competencies of their relevant teams, and on the performance in regard to 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 the claims by social media companies, and ensure oversight credibility, it is important to have a system that can independently monitor what is happening on the platforms. This means access to data at scale, as well as the analysis thereof. Since in most countries in Africa, social media companies cannot be legally compelled to disclose data in terms of existing laws, voluntary partnerships need to be sought in order to gain access to what is termed 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 contestation for elections. Therefore EMBs as electoral umpires can build confidence in their oversight role by demonstrating to voters that they are on top of what's happening on the platforms and are in liaison with the private powers that control these platforms in order to ensure a peaceful and positively informed electoral climate.

Underlying foundations:

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

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

Anything else specifically? AU data policy framework? ;

Annex:

Relevant clauses from the Foundational documents (to be elaborated) for all 3 actionables. Table format

	Instrument	Clause/s
Action 1: Demand disclosure from social media companies	AAEA Principles and Guidelines	Clause 9.6 All parties have a duty to comply with legislation on privacy and personal data protection throughout the electoral cycle and using the following international data protection standards: (a) Purpose limitation (b) Fairness, lawfulness and transparency (c) Data minimisation (d) Storage limitation (e) Accuracy (f) Confidentiality and integrity (g) Accountability Clause 9.7 The state should require digital and social media to have structures and processes for reporting action related to election integrity, including for content curation and moderation, user appeal and redress. Clause 11.1 In line with the United Nations' Guiding Principles on Business and Human Rights (UNGPs), the digital and social media must put in place processes for human rights due diligence and human rights impact assessment to identify, prevent, mitigate and account for how they address their impacts on human rights during the electoral cycle, and disclose these processes for transparency and accountability.

		Clause 11.4 (to be read with sub-clauses) Social media operators should provide information that is clear, understandable and accessible during the entire electoral cycle… Clause 11.5 Social media operators should be transparent and accountable about their corporate policies concerning elections, their content curation, and moderation measures and capacity in local languages, and should work with the media, civil society, EMBs and other key actors to publicise their content curation and moderation standards and reporting mechanisms for potentially harmful electoral-related content. … Clause 11.13 Recommender systems must not process any data that can be associated with a person and that could categorise their sensitive personal characteristics, including the following categories of information: (a) Religious or philosophical beliefs (b) Race or ethnic origin (c) Trade union membership (d) Political persuasion (e) Health or sex life (exception in Clause 11.14, and conditions of data sharing in Clause 11.15) Clause 11.16 The use of Artificial Intelligence should be transparent. People must be informed when they are interacting with an AI system, unless the context makes this obvious Relevant to EMBs: Clause 12.5 Data protection supervisory authorities should take active roles in relation to elections in upholding citizens' privacy and data protection rights during the entire electoral cycle, and should build on the Malabo Convention 2014 and other international standards to draw up appropriate safeguarding measures.
	Malabo Convention	Article 2.2, Scope of application Article 13, Principle 5 - Transparency of data processing Article 16, Right to Information Article 17, Right of Access

| | ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019 | Part III: Right of Access to Information

Principle 26. The right of access to information

1. The right of access to information shall be guaranteed by law in accordance with the following principles:

a. Every person has the right to access to information held by public bodies expeditiously and inexpensively.

b. Every person has the right to access information of private bodies that may assist in the exercise or protection of any right expeditiously and inexpensively.

Principle 28. Maximum disclosure

The right of access to information shall be guided by the principle of maximum disclosure. Access to information may only be limited by narrowly defined exemptions, which shall be provided by law and shall comply strictly with international human rights law and standards.

Principle 30. Duty to create, keep, organise and maintain information

Public bodies, relevant private bodies and private bodies shall create, keep, organise and maintain information in a manner that facilitates the exercise of the right of access to information.

Principle 31. Procedure for accessing information

1. Access to information shall be granted as expeditiously and inexpensively as possible, and in accessible formats and technologies.

2. No one shall be required to demonstrate a specific legal or personal interest in the information requested or to provide justification for a request.

3. Every person shall be assisted in making requests for information orally or in writing and in conformity with processing requirements. Appropriate support shall be provided to non-literate persons and persons with disabilities to make requests for information on an equal basis with others.

4. No fees shall be payable other than the reasonable reproduction cost of requested information. The cost of reproduction shall be waived where the requester is indigent.

5. Any refusal to disclose information shall be provided timeously and in writing, and it shall be well-reasoned and |

premised on international law and standards.

Principle 32. Appeals

Any refusal to disclose information shall be subject to an expeditious internal appeal process at no cost to the applicant. The right of further appeal against the outcome of an internal appeal process shall lie to the oversight mechanism and, ultimately, the courts.

Principle 33. Exemptions

1. Information may only be legitimately withheld where the harm to the interest protected under the relevant exemption demonstrably outweighs the public interest in disclosure of the information. Such information may only be withheld for the period that the harm could occur.

The detailed grounds for exemptions are spelled out in the Declaration.

Principle 36. Sanctions

1. The failure of an information holder to proactively disclose information or to grant a request for information shall be established as offences punishable by law.

2 The wilful destruction, damage, alteration, concealment or falsification of information and the obstruction or interference with the performance of the duties of an information holder or of an oversight mechanism, shall be established as offences punishable by law.

Part IV: Freedom of Expression and Access to Informa- tion on the Internet

Principle 39. Internet intermediaries

3. States shall require internet intermediaries to ensure that in moderating or filtering online content, they mainstream human rights safeguards into their processes, adopt mitigation strategies to address all restrictions on freedom of expression and access to information online, ensure transparency on all requests for removal of content, incorporate appeal mechanisms, and offer effective remedies where rights violations occur.

6. States shall ensure that the development, use and application of artificial intelligence, algorithms and other similar technologies by internet intermediaries are compatible with international human rights law and standards, and do not infringe on the rights to freedom of expression, access to

			information and other human rights.
	ACHPR Guidelines on Access to Information and Elections in Africa, 2017		Rationale and objectives of the Guidelines

The Guidelines provide direction to stakeholders in the electoral process who have a responsibility to proactively disclose various categories of information in their possession or control that are necessary for safeguarding the integrity and legitimacy of the electoral process. Guidance is provided in relation to the following stakeholders:

(a) Authorities responsible for appointing the Election Management Bodies;

(b) Election Management Bodies;

(c) Political Parties and Candidates;

(d) Law Enforcement Agencies;

(e) Election Observers and Monitors;

(f) Media and Online Media Platform Providers;

(g) Media Regulatory Bodies; and

(h) Civil Society Organisations.

Acknowledging the challenges of limited access to information during the electoral cycle which may foster public distrust, abstention and violence in the electoral process

Definitions

'Information' includes any original or copy of documentary material irrespective of its physical characteristics, such as records, correspondence, fact, opinion, advice, advertisement, memorandum, data, statistic, book, drawing, plan, map, diagram, photograph, audio or visual record, and any other tangible or intangible material, regardless of the form or medium in which it is held, in the possession or under the control of the information holder to whom a request has been made under these Guidelines.

'Relevant private body' refers to a body that would otherwise be a private body but is owned partially or totally, or controlled or financed, directly or indirectly, by public funds, or a body that carries out a statutory or public function or a statutory or public service.

General Principles |

The Right of Access to Information

2. The right to information is guaranteed in accordance with the following principles:

(b) Every person has the right to access information of private bodies that may assist in the exercise or protection of any right expeditiously and inexpensively.

(c) Any policy or practice creating a right of access to information shall be interpreted and applied on the basis of a duty to disclose. Non-disclosure shall be permitted only in exceptionally justifiable circumstances.

(d) No one shall be subject to any sanction for releasing information in good faith

Proactive Disclosure

3. The presumption is that all information held by relevant electoral stakeholders is subject to full disclosure. Accordingly, relevant electoral stakeholders are obliged to publish key information of public interest about their structure, functions, powers, decision making processes, decisions, revenue and expenditure in relation to the electoral process.

Duty to Create, Keep, Organise and Maintain Information

4. All relevant electoral stakeholders are obliged to create, keep, organise, maintain and manage information about the electoral process in machine-readable formats and in a manner that facilitates the right of access to information. This requires that electoral stakeholders keep and record information for a reasonable period of time on electoral cycle activities, and arrange this information in a manner that allows prompt and easy identification and also safeguards the integrity of its content

Procedure for Accessing Information

5. The process for accessing information held by relevant electoral stakeholders shall be simple, quick and affordable. In accessing information, no fees, other than the actual cost of reproduction, shall be charged. The cost of reproduction shall however be waived where the requester is indigent.

6. Any refusal of information by relevant electoral stakeholders shall be well reasoned and premised on existing regional and international standards and best practices on access to information. The refusal shall also be provided timeously, in writing and be subject to an internal appeal process which shall be expeditious and inexpensive The right of further appeal

		against the outcome of an internal appeal process shall lie to an independent body and the Courts.

Exemptions

7. The right to access information held by relevant electoral stakeholders may only be limited by narrowly defined exemptions, which shall be provided by law and shall comply strictly with regional and international standards and good practices on access to information.

The detailed grounds for exemptions are spelled out in the Guidelines.

Public Interest Override

9. Information can only be legitimately withheld by relevant election stakeholders where the harm to the interest protected under the relevant exemption clearly outweighs the public interest in disclosure of the information.

Whistleblowing Protection

11. Persons who, in good faith and in the public interest, disclose information about wrongdoing in the electoral process by a relevant electoral stakeholder or its employees, shall be protected from administrative, social, legal and employment-related sanctions or other sanctions of a similar nature. |
| | The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies ([A/HRC/50/56](#)) | **The part on: Corporate responsibility to respect human rights (pillar II)** |

| | | UN Guiding Principles on Business and Human Rights | Possibly, the EMBs can rely on this provision of the Guiding Principles on Business and Human Rights In their liaison with social media companies:

21. In order to account for how they address their human rights impacts, business enterprises should be prepared to communicate this externally, particularly when concerns are raised by or on behalf of affected stakeholders. Business enterprises whose operations or operating contexts pose risks of severe human rights impacts should report formally on how they address them.

The Commentary states that:

The responsibility to respect human rights requires that business enterprises have in place policies and processes through which they can both know and show that they respect human rights in practice. Showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors.

Communication can take a variety of forms, including in-person meetings, online dialogues, consultation with affected stakeholders, and formal public reports. Formal reporting is itself evolving, from traditional annual reports and corporate responsibility/sustainability reports, to include online updates and integrated financial and non-financial reports.

Formal reporting by enterprises is expected where risks of severe human rights impacts exist, whether this is due to the nature of the business operations or operating contexts. The reporting should cover topics and indicators concerning how enterprises identify and address adverse impacts on human rights. Independent verification of human rights reporting can strengthen its content and credibility. Sector-specific indicators can provide helpful additional detail. |
| | | UNESCO Guidelines for the Governance of Digital Platforms | *The responsibilities of digital platforms to respect human rights*

30. Digital platforms should comply with **five key principles**:

   a. **Platforms conduct human rights due diligence**, assessing their human rights impact, including the gender and cultural dimensions, evaluating the risks, and defining the mitigation measures.

   b. **Platforms adhere to international human rights standards, including in platform design, content moderation, and content curation.** Platforms should follow relevant international human rights standards, including the UN Guiding Principles on Business and Human Rights. Design should ensure non-discrimination and equal treatment and that harm is prevented; content moderation and curation policies and practices should be consistent with human rights standards, whether these |

practices are implemented through automated or human means, with knowledge of local languages and linguistic context as well as respect for cultural diversity, and adequate protection and support for human moderators.

c. **Platforms are transparent** and open about how they operate, with understandable and auditable policies as well as multistakeholder-designed metrics for evaluating performance. This includes transparency about the tools, systems, and processes used to moderate and curate content on their platforms, including in regard to algorithmic decisions and the results they produce.

d. **Platforms make information accessible** for users to understand the different products, services, and tools provided, and to make informed decisions about the content they share and consume. Platforms provide information and enable users' actions in their own languages and consider users' age and disabilities.

e. **Platforms are accountable to relevant stakeholders**— including users, the public, and actors within the governance system—in implementing their terms of service and content policies. They give users the ability to seek appropriate and timely redress against content-related decisions, including both users whose content was taken down or moderated and users who have made complaints about content.

31. Platforms should apply these principles in every jurisdiction where they operate, ensuring necessary resources and capacities to timely and effectively serve users.

32. To follow these principles, there are specific areas on which digital platforms have a responsibility to report or act before actors within the governance system, in accordance with international human rights standards. These areas are described in paragraphs 85–129 of the Guidelines.

Principles of governance systems

47. First, transparency should be a common overarching principle. In all governance systems, digital platforms are expected to be transparent about the terms, systems, and processes they use to moderate and curate content on their platforms, as well as on any human rights due diligence in line with the provisions of these Guidelines and the UN Guiding Principles on Business and Human Rights. They should be able to explain how their systems and processes fulfil their terms of service and effective implementation thereof, and if these are consistent with human rights international standards.

50. Third, governance processes should be open and accessible to all stakeholders, particularly the groups impacted by a proposed structure or type of regulation. Public consultations, open hearings, and online platforms should be utilized to provide

opportunities for public input and feedback. The concerns of groups in situations of vulnerability and marginalization, as well as women and girls, should be adequately represented in the decision-making process.

Data access for research purposes

116. Digital platforms should provide vetted researchers with access to non-personal data and pseudonymous data that is necessary to understand the impact of digital platforms. This data should be made available upon request and on an ongoing basis through automated means, such as application programming interfaces (APIs), or other open and accessible technical solutions allowing the analysis of said data.

117. Digital platforms are expected to provide access to non-personal data to journalist and advocacy groups when there is a public interest and the access is proportionate and necessary in a determined context. There need to be additional safeguards to protect users' privacy and personal data—such as ensuring anonymizing datasets through different measures, including de-identification and sampling before sharing—as well as businesses' proprietary information, trade secrets, and respect of commercial confidentiality.

118. Platforms should build reliable interfaces for data access and should provide disaggregated data based on gender and other relevant intersecting factors (such as race, ethnicity, age, socioeconomic status, disability, etc.). The governance system should determine what is useful, proportionate, and reasonable for research purposes.

Specific measures for electoral integrity

131. Digital platforms should recognize their role in supporting democratic institutions by preserving electoral integrity. They should establish a specific risk assessment process for the integrity of the electoral cycle in the lead-up to and during major national election events, significant regional elections, or constitutional referendums (for instance, for the legislature or head of state in a presidential system).

132. These assessments must be transparent, in line with human rights due diligence, and carried out with input from all relevant electoral stakeholders. The assessments should be conducted ahead of the electoral events in order to implement concrete measures to mitigate the identified risks. Assessments should include a gender approach, given the rise of online violence against women voters, candidates, activists, elected representatives, and electoral management officials.

133. Digital platforms should make a reasonable effort to ensure that users have access to information and ideas of all kinds according to international human rights law. In particular, they should ensure that automated tools do not hinder access to election-related content and diverse viewpoints.

141. Platforms should retain these advertisements and all the relevant information on funding in a publicly accessible and regularly updated online library.

| | CEDAW | *Article 2*

States Parties condemn discrimination against women in all its forms, agree to pursue by all appropriate means and without delay a policy of eliminating discrimination against women and, to this end, undertake:

(a) To embody the principle of the equality of men and women in their national constitutions or other appropriate legislation if not yet incorporated therein and to ensure, through law and other appropriate means, the practical realization of this principle;

(b) To adopt appropriate legislative and other measures, including sanctions where appropriate, prohibiting all discrimination against women;

(e) To take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise;

Part II, Article 7

States Parties shall take all appropriate measures to eliminate discrimination against women in the political and public life of the country and, in particular, shall ensure to women, on equal terms with men, the right:

(a) To vote in all elections and public referenda and to be eligible for election to all publicly elected bodies;

(b) To participate in the formulation of government policy and the implementation thereof and to hold public office and perform all public functions at all levels of government;

(c) To participate in non-governmental organizations and associations concerned with the public and political life of the country. |
| | Addis Ababa Declaration | Call on journalists, media outlets, electoral practitioners, Internet intermediaries and social media practitioners to:

Improve the transparency of internet companies' terms of service and other policies, in relation both to their content and the way these are applied in practice, and put in place systems which respect due process guarantees, including, where appropriate, by establishing independent external oversight mechanisms;

Call on each UNESCO Member State, including their Electoral Management Bodies, to: Adopt and/or implement right to information laws and policies and the required mechanisms to give effect to them, as per Sustainable Development Goal 16.10

Call on journalists, media outlets, electoral practitioners, Internet intermediaries and social media practitioners to: |

		Work to ensure that the public is provided with a diverse range of accurate information about parties, candidates and issues, and about any efforts to manipulate or influence the election, so that voters can make informed electoral choices Develop guidelines and policies for the use of artificial intelligence tools in content creation and distribution by media organisations and internet companies, taking into account the impact that this form of automation may have on freedom of expression and human rights in general; Improve the transparency of internet companies' terms of service and other policies, in relation both to their content and the way these are applied in practice, and put in place systems which respect due process guarantees, including, where appropriate, by establishing independent external oversight mechanisms;
Action 2 Monitoring partnerships	AAEA Principles and Guidelines	Clause 10.2 Throughout the electoral cycle, EMBs should deepen their internal capacity to understand and effectively use digital and social media, while partnering with relevant research and academic stakeholders to monitor and understand the technologies Clause 10.3 EMBs should have transparent cooperation agreements with digital and social media, focused on protecting the digital rights of users. Clause 10.4 EMBs should develop partnerships, mechanisms and capacities to monitor the digital and social media throughout the electoral cycle through relevant partnerships and collaborations with regulatory bodies, including monitoring adherence by candidates and parties to the guidelines on the use of digital and social media in elections. Clause 10.6 EMBs should facilitate and monitor the implementation of these Guidelines, on such aspects as sources and levels of advertising funds applicable to digital outputs, the nature of adverts, the advert's beneficiaries, the targeting methodology and the transparency of "adtech" companies about political advertisements. Clause 10.13 EMBs and oversight bodies should work with the media, academia, civil society organisations, social media and security forces to detect challenges arising from digital and social media

		that could threaten the electoral process before they occur, and develop risk mitigation strategies to address them. Clause 11.5 Social media operators should provide effective systems of vetted access to data for research purposes as relevant to electoral integrity.
	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	No clauses specifically relevant to monitoring.
	ACHPR Guidelines on Access to Information and Elections in Africa, 2017	No clauses specifically relevant to monitoring.
	UNESCO Guidelines for the Governance of Digital Platforms ...	***Accountability and Compliance*** 56. Regulatory arrangements should be effective and sustainable, taking into account the available local resources and the main priorities needing attention (for example, whether to address primarily issues around elections, public health, advertising, or data protection, etc.). Independent oversight is needed for all forms of regulation. The process for developing regulation should be open, transparent, and evidence-based. 57. Digital platforms deemed non-compliant with their own policies or failing to fulfill their duties to safeguard freedom of expression and access to information while dealing with content that could be permissibly restricted under international human rights law and standards, in accordance with the five principles described in paragraphs 85–129, should be held accountable to relevant bodies within the governance system and subject to proportionate enforcement measures with necessary procedural safeguards. 58. Self-regulation systems can be complementary and converge with other forms of regulation. They should include independent periodic mandatory audits that assess digital platforms' compliance with self-regulatory codes, policies, or norms. Such audits should not be directly funded by the industry or individual digital platforms, although levies on these entities can help cover the costs of such exercises. Nor should audits be conducted by any person or entity that would have or appear to have a conflict of interest. The terms and the results of the audit should be available for public comment.

		59. Co-regulatory structures should provide a legal framework that enables the environment for freedom of expression, access to information, and other human rights. In co-regulation, the regulatory role should be shared between industry and other stakeholders, and the government or the official independent regulatory authorities or bodies. The role of the relevant public authorities includes recognition of the co-regulatory scheme, auditing of processes, and funding the scheme (possibly through levies on platforms). Co-regulation should allow for the possibility of state-enforced penalties like fines, in the event that agreed objectives are not being met. 60. Statutory regulation of digital platforms addressing issues that might impact freedom of expression should be considered only when there is independence in decision-making of the regulatory authorities involved in its implementation. Such regulation should focus on systems and processes for content moderation and curation, rather than determining the legality of individual pieces of content, and must have a basis in law (i.e., be sufficiently defined), pursue a legitimate aim under Article 19 (3) of the ICCPR, and be necessary and proportionate. *Media and information literacy* **82.** Platforms should train their product development teams on media and information literacy, including online safety, from a user empowerment perspective and based on international standards, and put in place both internal and independent monitoring and evaluation mechanisms. *User reporting* **123.** Platforms should establish reporting mechanisms for users and non-users, or third parties representing their interests, so they can report potential policy violations. Effective and accessible complaints mechanisms should be in place for members of groups in situations of vulnerability and marginalization. Digital platforms should also have the means to understand local contextual conditions when responding to user complaints, ensuring a culturally sensitive system design. Special reporting mechanisms should be established for children, designed for quick and easy use. *Specific measures for electoral integrity* **135.** Digital platforms should make a reasonable effort to address content that could be permissibly restricted under international human rights law and standards, during the electoral cycle. Promoting independent fact-checking, advertisement archives, public alerts, and other measures should be taken into consideration. Engagement with relevant official independent regulatory institutions may be necessary according to the particular circumstances of each jurisdiction. **136.** Digital platforms should, as relevant, be transparent about the use and practical impact of any automated tools they use, albeit not necessarily the specific coding by which those tools operate, including inasmuch as those tools affect data harvesting, targeted advertising, and the sharing, ranking, and/or removal of content, especially election-related content.
	Addis Ababa Declaration	Carry out independent analysis of disinformation campaigns during election processes and their impact on elections

		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;
Action 3: Communicate	AAEA Principles and Guidelines	Clause 10.2.2 EMBs are encouraged to maintain a presence on social media as permitted by law, and keep their presence as up to date and responsive as possible to avoid information gaps. This presence should be conducted with the highest standards of cyber security, including the use of strong passwords and encryption where relevant Clause 10.14 EMBs should consider developing strategies and action plans to harness the benefits and respond to misinformation and other harm arising from digital and social media. These strategies should ensure that the election is not undermined by online harm throughout the election cycle.
	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	No clauses specifically relevant to communications
	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	*Principle 3. Platforms are transparent* 111. Digital platforms should regularly report to the public and the governance system on how they adhere to the principles of transparency and explicability, and how they perform relative to their terms of services and community standards. This includes their responses to government demands for information or content removal.[39] The implementation of this provision may need to vary in practice based on company size, to limit the burden on smaller companies and start-ups.

			112. Transparency should be meaningful—the information provided should be as clear and concise as possible, and as detailed and complex as necessary. Transparency is not simply the provision of legal texts or a data dump, but about providing stakeholders with the information they need to make informed decisions. *Language and accessibility* **119.** Platforms should have their full terms of service available in the official and primary languages of every country where they operate, ensure that they are able to respond to users in their own language and process their complaints equally, and have the capacity to moderate and curate content in the user's language. Automated language translators can be deployed to provide greater language accessibility but should be monitored for accuracy due to their technical limitations. **120.** Platforms should ensure that reports, notices, and appeals processes are available in the language in which the user interacts with the service. *Specific measures for electoral integrity* **137.** Digital platforms should also engage with all relevant stakeholders and their governance system prior to and during an election, to establish a means of communication if concerns are raised by the administrator or by users/voters. Engagement with relevant official regulatory institutions may be necessary according to the particular circumstances of each jurisdiction. **138.** Digital platforms that accept advertising designed to impact the electoral cycle should clearly identify such content as political advertisements. Digital platforms' terms of service should be clear about the digital platform's responsibility to be transparent about the amount of funding, the entity providing the funds, and the advertised entity, and consistently apply equal content moderation and curation rules on such advertisements. **139.** Digital platforms should track the monetization of posts by political parties and individuals representing parties.
		Addis Ababa Declaration	Invest in Media and Information Literacy among the general public, with a particular focus on the youth, in various ways, including by incorporating these competencies into formal, informal and non-formal education programmes Foster and use academic and scientific research on social media and social messaging effects, as well as safety of journalists, in order to guarantee that institutional and state responses are based on rigorous and extensive public analysis; Convinced that respect for the public's right to information, the expansion of Media and Information Literacy, and ensuring the safety of journalists, with cognisance of the particular threats to women journalists, and others exercising their right to freedom of expression, are key to addressing current

			challenges to elections;
	Guidelines for the governance of digital platforms: safeguarding FOE & ATI through a multi-stakeholder approach		Under the "Governance system" 42: The digital governance ecosystem consists of an array of diverse stakeholders, bodies, and regulatory arrangements throughout the world. While some existing governance systems, such as in the case of elections or data protection, should be interpreted and considered in accordance with the changes and challenges that the digital age entails, new governance systems are also being created in various contexts to directly regulate digital platforms. In any case, these regulatory mechanisms might have profound implications for freedom of expression and access to information and diverse cultural content online. Under "Principles of governance systems": 52: 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. Under "Use of automated systems for content moderation and curation": 107: Digital platforms should be able to explain to the governance system about the use and impact of the automated systems, including the extent to which such tools affect the data collection, targeted advertising, and the disclosure, classification, and/or removal of content, including artistic and election-related content. 112: Transparency should be meaningful—the information provided should be as clear and concise as possible, and as detailed and complex as necessary. Transparency is not simply the provision of legal texts or a data dump, but about providing stakeholders with the information they need to make informed decisions. 113: The transparency standards presented in these Guidelines can be considered as a minimum that should be met by all companies within the scope of any governance system. 115: Transparency on digital platforms' advertising practices m.Practices of advertising and data collection and results of the human rights and gender impact assessment of the advertising systems. Data access for research purposes 116. Digital platforms should provide vetted researchers with access to non-personal data and pseudonymous data that is necessary to understand the impact of digital platforms. This data should be made available upon request and on an ongoing basis through automated means, such as application programming

		interfaces (APIs), or other open and accessible technical solutions allowing the analysis of said data.
		117. Digital platforms are expected to provide access to non-personal data to journalists and advocacy groups when there is a public interest and the access is proportionate and necessary in a determined context. There need to be additional
		safeguards to protect users' privacy and personal data—such as ensuring anonymizing datasets through different measures, including de-identification and sampling before sharing—as well as businesses' proprietary information, trade secrets, and respect of commercial confidentiality.
		118.Platforms should build reliable interfaces for data access and should provide disaggregated data based on gender and other relevant intersecting factors (such as race, ethnicity, age, socioeconomic status, disability, etc.). The governance system should determine what is useful, proportionate, and reasonable for research purposes.

B. Implementation Guidance For Political Actors (parties, groups and independent candidates) on access to data in relation to elections

<u>Purpose and use of this guideline</u>

Data, especially that used by social media but also that 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 data is also the fuel of machine-learning AI. It can also help understanding Technology-Facilitated Gender-Based Violence, particularly for women candidates, women members of political parties, political groups and independent candidates- but also women in polling centres, working for EMBs or even women voters.

Therefore the focus here is on how political actors contesting African elections can get a greater understanding of the value of data in a national poll, so they can act as needed. It pinpoints the actions needed for this, elaborates on what these entail, and provides the legitimation in a range of agreed pan-African and international standards.

<u>Key action points/opportunities:</u>

1. **Transparency**: Urge platform companies that their databases should increase transparency in political advert spending and targeting; urge government to disclose data on spending (eg. on public advertisements, electoral subsidies; misuse of public infrastructure by the ruling party) as can be relevant to elections.
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 issue a public declaration refraining from use of digital disinformation and AI-fakes which are powered by data exploitation, and give access to their own data.

<u>What's entailed in each Action point:</u>

1. Transparency: Political advertising on social media can take place below the radar, as a result of customised adverts seen only by different audiences, and a lack of transparency about the variations, the targeting, reach and spend. This means each party may be relatively in the dark about what its rivals are doing online. 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, and come to the realisation that other adverts in the name of a political party are likely to be fake. On the question of government spending, political parties have an interest in a fair playing field, and monitoring potential bias by the authorities. This can be assessed through accessing data about government spending which can be clearly linked to election issues.
2. Empowerment: Parties have an interest in voters being well-informed about how social media works, in terms of how data, algorithmic systems and co-ordinated campaigning, can combine to boost virality. Voters should also be aware of data-driven micro-targeting of content and advertising, and be able to recognise when they are in a closed political bubble. The social media companies have the ability to reach every voter with messages, and short courses that can raise media and information literacy levels in regard to 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 which contaminate the 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 give access to data about their campaigns and spending. Transparency is also needed for candidates who could be paying directly to the platforms or for third actors paying for those candidates or parties and the companies where this is evidently electoral campaigning.

Underlying foundations:

1. Principles and Guidelines on the Use of Digital and Social Media
2. Declaration of principles of freedom of expression and access to information in Africa.
3. Guidelines on Access to Information in Times of Elections
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

Annex:

Relevant clauses from the Foundational documents

Action	Instrument	Clause/s
Action 1: Transparency	AAEA Principles and Guidelines	2.2.6.2 Micro targeting is a form of online targeted advertising that analyses personal data to identify the interests of a specific audience or individual to influence their actions. Micro targeting may be used to offer a personalised message or personalised content to an individual or targeted audience using an online service such as social media. 11.4 Social media operators should provide information that is clear, understandable and accessible during the entire electoral cycle regarding the following: 11.4.1 Political advertising, including information relating to the political advertisements themselves, the origin and the funding of such advertisements and a repository of such advertisements 11.15 A person may consent to the use of their data for advertising by a specific digital or social media entity. In this case, the digital service provider should completely anonymise that data before sharing it with any other entity (including entities within the same company) so that it can never be linked to that person again. 12.7 Regulatory bodies should develop regulations to deal with political microtargeting and online political advertising. These regulations should govern what candidates and political parties can do and the obligations of digital and social media.

	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	Principle 41. Privacy and communication surveillance 1. States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications. 3. States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including: a. the prior authorisation of an independent and impartial judicial authority; b. due process safeguards; c. specific limitation on the time, manner, place and scope of the surveillance; d. notification of the decision authonsing surveillance within a reasonable time of the conclusion of such surveillance; e. proactive transparency on the nature and scope of its use; and f. effective monitoring and regular review by an independent oversight mechanism.
	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	**Principle 3. Platforms are transparent** **111.** Digital platforms should regularly report to the public and the governance system on how they adhere to the principles of transparency and explicability, and how they perform relative to their terms of services and community standards. This includes their responses to government demands for information or content removal.[39] The implementation of this provision may need to vary in practice based on company size, to limit the burden on smaller companies and start-ups. **112.** Transparency should be meaningful—the information provided should be as clear and concise as possible, and as detailed and complex as necessary. Transparency is not simply the provision of legal texts or a data dump, but about providing stakeholders with the information they need to make informed decisions. **113.** The transparency standards presented in these Guidelines can be considered as a minimum that should be met by all companies within the scope of any governance system. *Meaningful transparency* **114.** The effectiveness of digital platforms' transparency mechanisms should be independently evaluated against international standards through qualitative and empirical quantitative assessments to determine whether the information provided for meaningful transparency has served its purpose. Reports should be made publicly available on a regular basis.

115. Digital platforms should publish information outlining how they ensure that human rights and due process considerations are integrated into all stages of the content moderation and curation policies and practices. This publicly available information should include:

Transparency in relation to digital platforms' terms of service

a. Any measures used to moderate and curate content, set out in platforms' terms of service, including, for instance, lists of banned content or users.

b. Any information about processes used to enforce their terms of service and to sanction users, as well as government demands/requests for content removal, restriction, or promotion.

c. Information about the reasons behind restrictions imposed in relation to the use of their terms of service should be publicly available in an easily accessible format in their terms of service.

d. Information about the types of content that are considered prohibited or against which the digital platform will act under their terms of service, and the measures taken, including the circumstances under which the digital platform will suspend a user's account, whether permanently or temporarily.

Transparency in relation to the implementation of content moderation and curation policies and practices

e. How content is moderated and curated, including through automated means and human review, as well as content that is being removed or blocked under either terms of service or pursuant to government demands/requests. This should include quantitative and qualitative information about the actual outcomes, results, and impacts that these systems produce.

f. Anychangeincontentmoderationandcurationpoliciesshouldbecommunicated in accessible formats to users periodically.

g. Any use made of automated means for the purpose of content moderation and curation, including a specification of the role of the automated means in the review process, and any indicators of the benefits and limitations of the automated means in fulfilling those purposes.

h. Any safeguards applied in relation to content moderation and curation that are put in place to protect freedom of expression and access to information and diverse cultural content—including in response to government requests—particularly in relation to matters of public interest, including journalistic, artistic, and cultural content, and intellectual property rights.

i. Informationaboutthenumberofhumanmoderatorsemployedorsub-contracted and the nature of their expertise in the local language(s) and local context, as well as whether they are in-house staff or contractors.

j. How personal data is collected, used, disclosed, stored, and shared, and what treatment is made of users' personal data, including which personal and sensitive data is used to make algorithmic decisions for the purpose of content moderation and curation. This also includes how personal data is shared with

		other entities and what personal data the platform obtains indirectly, for instance, through user profiling or interoperability with other parts of the digital ecosystem. Transparency in relation to user complaints mech **k.** Information relevant to appeals about the removal, blocking, or refusal to block content and how users can access the complaints process. This information should include quantitative and qualitative information of appeals received, treated, accepted, and rejected, and about the results of such appeals, and information about complaints received from State officials and the actions taken. Transparency on digital platforms' advertising practices **l.** For digital platforms that use advertising as part of their business model, information about political advertisements and those of public interest, including the author and those paying for the ads, should be retained in a publicly accessible library online. **m.** Practices of advertising and data collection and results of the human rights and gender impact assessment of the advertising systems. **n.** Information which allows individuals to understand the basis on which they are shown particular advertising. **o.** Content generated exclusively by machines should be labelled as such.
	Addis Ababa Declaration	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;
Action 2: Empowerment	AAEA Principles and Guidelines	2.2.5 Media and information literacy, and digital literacy. Media and information literacy refers to the knowledge, attitudes and skills of people to engage critically and effectively with media technologies and institutions, and related content. In this context, digital literacy involves the specific competencies for using digital technologies. Both literacies are important for elections. 3.1.4 Relevant electoral stakeholders must take specific measures to address the needs of marginalised or vulnerable groups in a manner that guarantees the full enjoyment of fundamental rights on an equal basis with others, including in respect of access to digital and social media, the protection of safety online and the provision of media and information literacy. 10.11 EMBs should consider partnerships with relevant

		stakeholders to harness the youth potential as digital and social media creators and consumers, and empower them with media and information literacy skills, including digital dimensions, and voter education. 11.3 Social media operators should proactively contribute to elections by encouraging voter registration and voting by promoting sources of reliable and verified electoral information, and by supporting media and information literacy as relevant to elections. 11.9 Social media operators must take specific measures to address the needs of marginalised groups in a manner that guarantees the full enjoyment of fundamental rights on an equal basis with others, including in respect of access to online services, safety online, and media and information literacy and digital literacy
	Other instruments…	**Media and information literacy** 74. Media and information literacy covers a broad range of skills that allow users to think critically about the information they interact with online. Media and information literacy should be addressed specifically through the governance system to ensure that all stakeholders, including digital platforms, are effectively playing their part. 75. Media and information literacy will be most effectively achieved when stakeholders within the governance system share a common vision and work collaboratively to achieve it through sharing knowledge and resources. Media and information literacy programmes should be responsive to the availability of existing and emerging media and information technologies so that citizens can fully benefit from their use to actively participate in their societies. 76. Media and information literacy programmes should put an emphasis on the empowerment of users and ensure that they have the skills and knowledge that will enable them to interact with content critically and effectively in all forms of diverse media and with all information providers—including schools, universities, research institutions, libraries, archives, museums, media companies, publishers, statistical entities, and

		more. When media and information literacy programmes only emphasize protection or digital safety skills, they may lead to excessive restrictions placed on the use of digital platforms. However, they should prioritise specific steps that users can take, based upon best practices published by UNESCO and other international bodies, to identify content that could be permissibly restricted under international human rights law and standards.
		77. Media and information literacy programmes should promote cultural diversity, social inclusion, and global citizenship, and aim to reduce the "participation gap" between people who are engaged in the creation and critical use of media and information content and those who are not. Media and information literacy programmes should also promote gender equality and women's empowerment and provide opportunities for participation by groups in situations of vulnerability and marginalization.
		78. Governments should always consider the promotion of media and information literacy, including online safety skills, for users, especially all groups in situations of vulnerability and marginalization, as well as women and girls. This enables users to engage critically with content and technologies, navigate a rapidly evolving media and information landscape marked by digital transformation, promote human rights, and build resilience in the face of related challenges.
		79. Governments should disseminate information and conduct awareness-raising campaigns on the rights of the child in the digital environment, including their right to freedom of expression, focusing in particular on those whose actions have a direct or indirect impact on children. They should facilitate educational programmes for children, parents and caregivers, the general public, and policymakers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should include information on how children can benefit from digital products and services and develop their media and information literacy, including digital skills.
		80. Platforms should establish a clear and public strategy to empower users and promote a favorable online environment that safeguards freedom of expression and access to information through media and information literacy, including online safety education.

		There should be a specific focus within the digital platform on how to improve the digital literacy of all users, especially groups in situations of vulnerability and marginalization, with thought given to this in product development teams.
		81. Digital platforms should allocate adequate resources to improve media and information literacy of all users, including digital literacy about the platform's own products and services, as well as relevant processes. This should especially focus on improving users' understanding of the ways that a given platform presents, curates, recommends, and/or flags content (also connected to the steps outlined under Principles 3 and 4, below) and specific steps users can take to themselves identify content that could be permissibly restricted under international human rights law and standards.
		82. Platforms should train their product development teams on media and information literacy, including online safety, from a user empowerment perspective and based on international standards, and put in place both internal and independent monitoring and evaluation mechanisms.
		83. Both governments and digital platforms should implement media and information literacy programmes in close collaboration with organizations and diverse experts independent of the platforms, including but not limited to: public authorities responsible for media and information literacy, academia, civil society organizations working with groups in situations of vulnerability and marginalization, researchers, librarians, teachers, specialized educators, journalists, artists, and cultural professionals. Specific measures should be taken for users and non-users and audiences from groups in situations of vulnerability and marginalization, as outlined in the many UNESCO tools available on media and information literacy.
		84. Governments and digital platforms should collaborate and ensure that users understand their rights online and off-line, including the role of media and information literacy in the enjoyment and protection of the rights to freedom of expression and access to information.
	Addis Ababa	

	Declaration	
Action 3: Keeping it clean	AAEA Principles and Guidelines	9.6 … All parties have a duty to comply with legislation on privacy and personal data protection throughout the electoral cycle and using the following international data protection standards: (a) Purpose limitation (b) Fairness, lawfulness and transparency (c) Data minimisation (d) Storage limitation (e) Accuracy (f) Confidentiality and integrity (g) Accountability 13.2 Political parties and candidates should not commit, support, encourage or condone any form of potential online harm, including by their supporters during the entire electoral cycle, and should comply with relevant rules and standards. 13.3 Political parties and candidates should ensure that campaigns conducted on digital and social media, including messaging, are transparent and clearly attributed, including the use of paid-for-content, including influencers. 13.4 Political parties, political leaders, members and candidates should uphold data protection and protect fundamental rights, including voters' data protection rights.
	ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019	Principle 23. Prohibited speech 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.
	Other instruments…	
	Addis Ababa declaration	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; 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;
	UN Guiding Principles on Business and Human Rights	
	The practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies ([A/HRC/50/56](A/HRC/50/56))	
		138: Digital platforms that accept advertising designed to impact the electoral cycle should clearly identify such content as political advertisements. Digital platforms' terms of service should be clear about the digital platform's responsibility to be transparent about the amount of funding, the entity providing the funds, and the advertised entity, and consistently apply equal content moderation and curation rules on such advertisements. 139: Digital platforms should track the monetization of posts by political parties and individuals representing parties. 140: Platforms should disclose to the public information about the specific demographics targeted by such advertising/promotions. 14: Platforms should retain these advertisements and all the relevant information on funding in a publicly accessible and regularly updated online library.

C. Implementation guide for civil society on data access and elections

<u>Purpose and use of this guideline</u>

Data, especially that used by social media, 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 data is also the fuel of machine-learning AI.

Therefore the focus here is on how African civil society (including election observers, voter education groups, media, civic tech working in public interest, human rights defenders, academia) can get a greater understanding of the role of data in a national election, so they can intervene as needed. It pinpoints the actions needed for this, elaborates on what these entail, and provides the legitimation in a range of agreed pan-African and international standards.

<u>Key action points/opportunities for civil society:</u>

1. **Monitor**: Increase capacity to collect and assess data relevant in elections, including from social media, political parties and EMBs
2. **Collaborate**: Offer partnerships with EMBs and Tech companies to build this function for election integrity, and to monitor how platforms are responding to challenges and opportunities on their services
3. Use data access to **promote accountability** from political parties, EMBs and platforms, including for election disputes, and educate voters about the issues of data in the election, and why transparency and data access is important.

What's entailed in each action point:

1. Civil society constitutes an independent oversight role of what's happening on social media during elections, and what the platform companies are doing about it. But systematic monitoring is needed to detect patterns of content (including adverts) that could violate human rights essential to election integrity. It is also needed to see what the companies themselves are doing with regard to such threats, and with regard to the opportunities to promote positive content. However, civil society needs a range of methods to monitor all this (ranging through donated access to data by the companies; paid access (including via data broker firms; informal scraping; and targeted probabilistic sampling such as partnerships with groups subjected to harm - like women journalists).
2. Without compromising independence, civil society actors can optimise their data access, capacities and impact with structured relationships with EMBs and the tech 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 this into capacity building programmes for various stakeholders.

Underlying foundations:

1. [Principles and Guidelines on the Use of Digital and Social Media](#)
2. [Declaration of principles of freedom of expression and access to information in Africa](#).
3. [Guidelines on Access to Information in Times of Elections](#)
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](#)

Annex:

Relevant clauses from the Foundational documents

	Instrument	Clause/s
Action 1: Monitor	AAEA Principles and Guidelines	11.5 Social media operators should be transparent and accountable about their corporate policies concerning elections, their content curation, and moderation measures and capacity in local languages, and should work with the media, civil society, EMBs and other key actors to publicise their content curation and moderation

		standards and reporting mechanisms for potentially harmful electoral-related content. Social media operators should provide effective systems of vetted access to data for research purposes as relevant to electoral integrity.
	Other instruments (to be added) …	
	Addis Ababa Declaration	
Action 2: Collaborate	AAEA Principles and Guidelines	10.13 EMBs and oversight bodies should work with the media, academia, civil society organisations, social media and security forces to detect challenges arising from digital and social media that could threaten the electoral process before they occur, and develop risk mitigation strategies to address them
	Next instruments	
Action 3: Empower	AAEA Principles and Guidelines	15.1 Civil society organisations should engage with the state, EMBs, the digital and social media and other relevant electoral stakeholders to initiate and implement media and information, as well as digital literacy and fact-checking skills initiatives.
	Other instruments …	
	Addis Ababa Declaration	Foster and use academic and scientific research on social media and social messaging effects, as well as safety of journalists, in order to guarantee that institutional and state responses are based on rigorous and extensive public analysis;
Action: Research	UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-	Under The role of civil society and other stakeholders: 37. Researchers should be able to collect and analyse disaggregated data based on gender and other relevant intersecting factors (such as race, ethnicity, age, socioeconomic status, disability, etc.). This helps identify disparities, biases, and differential impacts of digital platforms on different groups in vulnerable and marginalized situations. 107. Digital platforms should be able to explain to the governance system about the use and impact of the

	stakeholder approach	automated systems, including the extent to which such tools affect the data collection, targeted advertising, and the disclosure, classification, and/or removal of content, including artistic and election-related content.
		112. Transparency should be meaningful—the information provided should be as clear and concise as possible, and as detailed and complex as necessary. Transparency is not simply the provision of legal texts or a data dump, but about providing stakeholders with the information they need to make informed decisions.
		Under transparency on digital platforms' advertising practices:
		115. (m) Practices of advertising and data collection and results of the human rights and gender impact assessment of the advertising systems.
		Data access for research purposes
		116. Digital platforms should provide vetted researchers with access to non-personal data and pseudonymous data that is necessary to understand the impact of digital platforms. This data should be made available upon request and on an ongoing basis through automated means, such as application programming interfaces (APIs), or other open and accessible technical solutions allowing the analysis of said data.
		118. Platforms should build reliable interfaces for data access and should provide disaggregated data based on gender and other relevant intersecting factors (such as race, ethnicity, age, socioeconomic status, disability, etc.). The governance system should determine what is useful, proportionate, and reasonable for research purposes.
		Under context-specific provisions:
		130. Digital platforms should put in place sufficient special protections for women and girls, users from groups in situations of vulnerability and marginalization, and journalists, artists, human rights defenders, and environmental defenders. To achieve this, digital platforms should:

		b) Use privacy-protecting technology to provide external researchers with access to the platforms' internal data to help identify algorithmic amplification of online gender-based violence or other trends of violence arising from emerging technologies. 136. Digital platforms should, as relevant, be transparent about the use and practical impact of any automated tools they use, albeit not necessarily the specific coding by which those tools operate, including inasmuch as those tools affect data harvesting, targeted advertising, and the sharing, ranking, and/or removal of content, especially election-related content. 140. Platforms should disclose to the public information about the specific demographics targeted by such advertising/promotions. 141. Platforms should retain these advertisements and all the relevant information on funding in a publicly accessible and regularly updated online library.
Action: Advocacy	UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach	117. Digital platforms are expected to provide access to non-personal data to journalists and advocacy groups when there is a public interest and the access is proportionate and necessary in a determined context. There need to be additional safeguards to protect users' privacy and personal data—such as ensuring anonymizing datasets through different measures, including de-identification and sampling before sharing—as well as businesses' proprietary information, trade secrets, and respect of commercial confidentiality. 118. Platforms should build reliable interfaces for data access and should provide disaggregated data based on gender and other relevant intersecting factors (such as race, ethnicity, age, socioeconomic status, disability, etc.). The governance system should determine what is useful, proportionate, and reasonable for research purposes.

		Under Specific measures for electoral integrity: 133. Digital platforms should make a reasonable effort to ensure that users have access to information and ideas of all kinds according to international human rights law. In particular, they should ensure that automated tools do not hinder access to election-related content and diverse viewpoints.
Action: Empower	UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach	26. Specifically, States should: 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 marginalization, and fulfil all women's and girls' right to access to information.
Action: Collaborate	UNESCO Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach	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.
Due diligence	UNGPs on business and human rights	**Principle 17.** In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human

		rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. **Principle 18**. In order to gauge human rights risks, business enterprises should identify and assess any actual or potential adverse human rights impacts with which they may be involved either through their own activities or as a result of their business relationships. *The UNGPs highlight the responsibility of states to protect human rights, including ensuring that businesses operating within their jurisdiction do not violate human rights. Civil society can advocate for robust national legal frameworks and regulations that govern data access and protect individuals' privacy. *Civil society organisations can also monitor companies involved in providing data-related services during elections, such as social media platforms or data analytics firms, so that they respect human rights throughout their operations. Transparency clauses: *CSOs, especially those focused on election monitoring and human rights advocacy, can use the principles to engage with both governments and private entities and advocate for transparent and accountable data practices, pushing for regulations that balance the need for information with the protection of privacy and freedom of expression.
Access to remedy	UNGPs on business and human rights	Principle 25. As part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy. Principle 27. States should provide effective and appropriate non-judicial grievance mechanisms, alongside judicial mechanisms, as part of a comprehensive State-based system for the remedy of business-related human rights abuse. *CSOs can play a pivotal role in advocating for individuals' rights and seeking remedies for any violations and advocate

		for the adoption of to address human rights abuses related to the access to data during elections.
Awareness and capacity building:	UNGPs on business and human rights	Principle 3: Under operational principles *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.
Multi-stakeholder engagement	UNGPs on business and human rights	Principle 3: Under operational principles *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.
Documentation and advocacy	UNGPs on business and human rights	Principle 3: Under operational principles Civil society can document and highlight instances where data practices impact human rights negatively. Through research, advocacy, and campaigns, CSOs can draw attention to potential abuses and press for corrective actions.