DIGITAL DEMOCRACY OR DATA EXPLOITATION:

MONITORING THE USE OF PERSONAL DATA IN ELECTIONS

A Guide for Nonpartisan Citizen Election Observers

National Democratic Institute (NDI)


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


Sida

ACKNOWLEDGEMENTS

Nonpartisan citizen election observers around the world face increasingly complex political and digital threats to credible elections, requiring them to observe for longer periods of time, cover more diverse processes, and use multiple methodologies and approaches to capture evolving dynamics. This is at a time when funding and resources for nonpartisan citizen observation worldwide is on the decline, making elections more vulnerable to exploitation or eroding public confidence. Transnational networks like the Global Network of Domestic Election Monitors (GNDEM) have continued to build solidarity and learning opportunities between and among citizen election observers around the globe during this challenging time. This guide was drafted in part in response to expressed interests by the GNDEM community.

The National Democratic Institute (NDI) is grateful to the Swedish International Development Cooperation Agency (Sida) for funding this valuable resource and supporting the work of citizen election observers. This guide was developed as part of a Sida-funded initiative geared at combatting digital threats to elections.

This guide was supported by an Advisory Group of citizen election monitoring leaders and experts in data protection and privacy and elections from all around the world. They include: Mahishaa Balraj (Hashtag Generation), Adam Buselau (European Platform for Democratic Elections), Tomaso Falchetta and Julie Reintjes (Privacy International), Iluri Lisovsky and Olha Kotsyuruba (OPORA), Zofia Lutkiewicz (Political Accountability Foundation), Amber Macintyre (independent expert), Heloisa Massaro (Internet Lab), Rasa Nedeljkov (CRTA), Jerry Sam (PenPlusBytes), and Alex Shlyk (independent expert). The outline and guidance from this guide was presented and reviewed by GNDEM representatives and experts in August 2025 in Nairobi, Kenya. NDI and GNDEM expresses their appreciation to all individuals and organizations who lent their expertise and insights in contributing to this guide.

This guide was written by Tetyana Bohdanova with support from Julia Brothers and Anis Samaali. The guide was reviewed by Richard Klein and other NDI experts including Nathan Grubman, Sef Ashiagbor, and Kellor Yde, as well as the Advisory Group.

INTRODUCTION

As campaigns become increasingly data-driven and powered by artificial intelligence (AI), democratic institutions face growing threats from the exploitation of personal data in electoral processes. Through massive data collection and processing, individuals are profiled based on their political views and characteristics, and precisely targeted with content designed to influence their opinions and behavior. Personal data has become a political commodity that can be bought, sold, traded, and sometimes stolen to influence elections and gain unfair advantages. These practices are often obscured from or not disclosed to voters and election observers, which weakens accountability among election participants.

Additionally, while election management bodies (EMBs) have always dealt with sensitive personal information, improvements in data systems, biometrics, and other election administration technology mean that election officials are collecting, processing, and storing large amounts of centralized personal information. This requires clear and open protections to ensure information is handled responsibly and securely, without being influenced by political pressure or bias. Privacy concerns, however, should not compromise transparency in election administration; interfere with efforts to make election data publicly available according to **open data principles**; or undermine the ability of election observers to assess election-related processes. There is a compounding challenge of autocrats using privacy arguments to undermine electoral transparency. As discussed throughout this guide, it is possible to both protect data and deliver transparent and accountable elections.

While much attention has been focused on the influence of social media on the electoral information environment, less scrutiny has been given to the underlying data collection and targeting infrastructure, including commercial data brokers, evolving data-driven campaign methods, and data-centered election technologies. Election observers increasingly need to examine these practices and technologies but face significant challenges in updating their methodologies and developing the necessary technical expertise.

At the same time, there is a growing movement to protect personal data and encourage transparency around its use in the digital age. Journalists, tech experts, academics, and civil society organizations have studied how personal data is used in political campaigns. There is an important opportunity for nonpartisan citizen election observers to learn from existing techniques to inform their approaches and methodologies and incorporate a data privacy and protection lens to their observation efforts.

This Guide aims to bridge this gap by equipping nonpartisan citizen election observers with the essential background knowledge, practical instruments, and analytical frameworks needed to integrate data protection considerations into their existing election observation methodologies, enabling a more comprehensive assessment of how personal data practices affect the conduct of democratic elections.

It builds upon existing groundwork already established by organizations working in technology research, data protection, and elections, including: the National Democratic Institute's 2024 ***Monitoring Electoral Electronic Technologies: A Model Checklist*** and its 2022 ***Recommendations for the Adoption of Electronic Electoral Technologies*** that provide comprehensive frameworks for assessing electronic voting and related technologies;

"**Principles and Guidance for Observing Personal Data Use in Elections**"[1] guidance document for the Declaration of Principles for International Election Observation community; Privacy International's 2023 ***Technology, Data and Elections: An Updated Checklist on the Election Cycle***, which offers valuable guidance on privacy considerations throughout electoral processes; and Tactical Tech's 2019 ***Personal Data: Political Persuasion: Inside the Influence Industry – How it works***, which illuminates the mechanisms through which personal data is leveraged for political influence.

The guide is structured to support nonpartisan citizen election observers in progressively building their understanding and capacity to monitor personal data use in elections. It begins by establishing the foundational "why" in Chapter 1, explaining the critical connection between data protection and election integrity, including how personal data protection relates to international electoral standards. Chapter 2 explains core data protection principles, data subject rights, and how privacy considerations complement rather than conflict with election transparency goals. Chapter 3 addresses the unique considerations and challenges citizen election observers may face when monitoring data protection issues. The guide then shifts to practical application in Chapter 4, which maps out how personal data flows through the election cycle – from voter registration and campaign activities to election day procedures – examining both election administration and campaign contexts separately with their distinct data practices, risks, and vulnerabilities. Chapter 5 walks observers through planning an observation effort from risk assessment and scope determination through method selection and communication strategies. Chapters 6 and 7 look beyond observation itself to address impact and advocacy, discussing how to formulate recommendations and engage in policy reform, before concluding with forward-looking considerations.

The guide is specifically designed for nonpartisan citizen election observers safeguarding their own electoral processes. It will focus on methodologies that are achievable and not resource-intensive, with additional guidance on how data protection can be integrated into pre-existing monitoring strategies.

The authors recognize that the Guide may also prompt citizen election observation organizations to reflect on and improve their own data handling practices. However, providing comprehensive recommendations on implementing data protection measures within election monitoring organizations falls outside the scope of this document, and observers are strongly advised to seek separate professional and legal guidance to ensure their own operations comply with applicable data protection laws and ethical standards.

1 Finalized at the 2025 annual Implementation Meeting: h**ttps://dop-elections.org/wp-content/uploads/2025/12/DoP-Data-Protection-Guidance-FINAL-June-2025.pdf**

CHAPTER 1: WHY SHOULD CITIZEN ELECTION OBSERVERS CARE ABOUT DATA PROTECTION AND PRIVACY?

PERSONAL DATA PROTECTION AS AN ELECTION INTEGRITY ISSUE

For over a decade, much civil society and media attention has focused on challenges posed to election integrity by malign information operations, while a lot less scrutiny has been given to the underlying infrastructure of data collection and targeting that enable distortion of the information landscape and, in less democratic context, voter surveillance, coercion, or suppression. Concurrently, a complex commercial ecosystem emerged, comprising a network of consultants, technology companies, and digital platforms that leverage personal data and data-driven technologies to influence public opinion and voter behavior.[2] Alongside this ecosystem, there is a growing number of tech vendors offering solutions heavily reliant on voter data for election administration at various stages of the electoral cycle.

At the same time, citizen election observers are already monitoring numerous aspects of the electoral process that are increasingly data-centric. From voter registration and voter identification systems to targeted political advertising, campaign finance, or the abuse of state resources, observers regularly encounter data-driven practices that can impact the integrity of the electoral process. Personal data has become a political capital just as much as financial donations or access to administrative resources, and can be misused by political or state actors for unfair electoral advantage. The increased proliferation of data-centric technology in both election administration and election campaigning, accelerated by the new AI-based tools, compels observers to incorporate data protection considerations into their ongoing observation methodologies. This will enable watchdogs to more thoroughly evaluate the most transformative – and potentially threatening – developments in the contemporary electoral landscape.

Citizen observers are also uniquely positioned to bridge the critical knowledge gap between the public, election officials, and electoral actors regarding how personal data is collected, processed, and deployed throughout the electoral cycle. By incorporating data protection frameworks into their observation methodologies, they can provide independent, expert assessments that, as appropriate, bolster public trust, ensure accountability in the adoption of new technologies, and deliver actionable recommendations for safeguarding both individual privacy rights and the fundamentals of election integrity.

2 For instance, Tactical Tech has identified and compiled a **database** of over 500 commercial vendors offering data-centered campaign technologies and services to political campaigns.

Right to Privacy and the International Electoral Integrity Standards

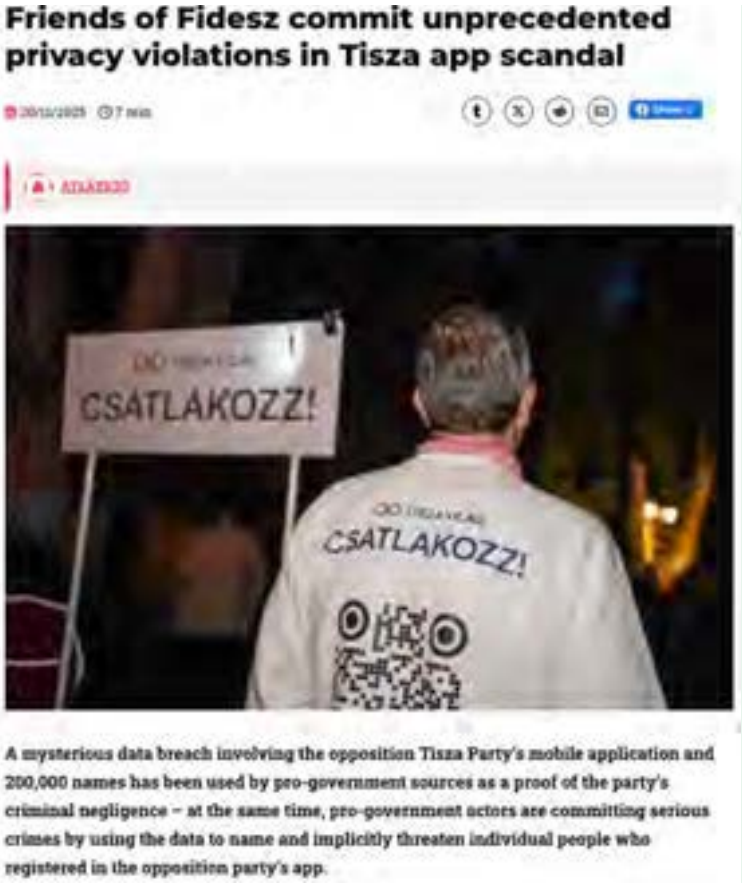
The Right to Privacy is a human right, recognized by various international and regional human rights instruments. Among them: Art.12 of the Universal Declaration of Human Rights,[3] Art.17 of the International Covenant on Civil and Political Rights (ICCPR)[4], the Council of Europe's Convention 108+[5], the EU General Data Protection Regulation (GDPR)[6], the Asia-Pacific economic cooperation (APEC) privacy framework,[7] the Organization of American States (OAS) guiding principles and recommendations for personal data protection laws, [8]the Organisation for Economic Co-operation and Development (OECD) guidelines on the protection of privacy,[9] the Convention on Cybercrime (Budapest Convention),[10] the African Union's Convention on Cyber Security and Personal Data Protection[11] as well as its Data Policy Framework, among others.

Data protection serves to uphold the fundamental right to privacy through regulation of how personal data is handled: it grants individuals control over their information and establishes accountability frameworks with defined responsibilities for those who manage or process the data. Moreover, in recent years, data protection has begun to be recognized as a standalone right.[12]

In order to be able to credibly assess data protection and privacy issues within the electoral process, it is important to understand how the application of existing data protection obligations in the electoral context could impact a number of election integrity standards. Among them:

- **The right to participate in elections freely and securely:** Universal suffrage, in addition to granting every citizen the right to vote and be elected in genuine, periodic elections, also guarantees secrecy of the vote, ensuring the free expression of the will of the voter.[13] Voters also have the right to seek, receive, and impart accurate information that allows them to make informed choices regarding their future, free from intimidation, violence, or manipulation.[14]

3 Article 12 of the Universal Declaration of Human Rights (**UDHR**).
4 Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).
5 Convention for the protection of individuals with regard to the processing of personal data (**Convention 108+**).
6 The EU General Data Protection Regulation (**GDPR**).
7 **APEC Privacy Framework**.
8 OAS **Updated Principles on Privacy and Personal Data Protection**.
9 OECD **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**.
10 The **Budapest (Cybercrime) Convention**.
11 **African Union's Convention on Cyber Security and Personal Data Protection**.
12 I.e., Article 8 of the **Charter of Fundamental Rights of the European Union** (2012/C 326/02); Article 7 of the Charter upholds the right to privacy.
13 Article 25 of the International Covenant on Civil and Political Rights (**ICCPR**).
14 "Persons entitled to vote must be free to vote for any candidate for election and for or against any proposal submitted to referendum or plebiscite, and free to support or to oppose government, without undue influence or coercion of any kind which may distort or inhibit the free expression of the elector's will. Voters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind." – General Comment 25, paragraph 19, UNHRC.



Friends of Fidesz commit unprecedented privacy violations in Tisza app scandal

A mysterious data breach involving the opposition Tisza Party's mobile application and 200,000 names has been used by pro-government sources as a proof of the party's criminal negligence – at the same time, pro-government actors are committing serious crimes by using the data to name and implicitly threaten individual people who registered in the opposition party's app.

In 2025, personal data of the 200,000 Hungarian opposition party Tisza's supporters ***was leaked from the party's mobile app*** *under obscure circumstances and subsequently publicized by pro-government political operatives as means of intimidation.*[15]

The security and proper handling of voter data has become a major vulnerability in electoral processes, particularly as EMBs increasingly adopt advanced data systems and biometric technologies for election administration, which poses significant risks of breaches, leaks, and unauthorized access – as evidenced by incidents affecting millions of voters in countries around the world.[16]

Furthermore, the rapid advancement of technologies like generative AI (genAI) threatens even more extreme personal data uses, including in ways that can infer or reveal political opinions. In less democratic contexts, unfettered personal data access can be exploited by authoritarian regimes to surveil and intimidate the opposition and independent civil society, while digital technology may be used to facilitate vote-buying and other irregular practices.

- **The right to participate and campaign for votes, alongside the right of voters to hold opinions and to seek and receive information in order to make an informed choice on election day:** Everyone has the right to form, hold, and change opinions without interference or manipulation, which is integral to freely exercising the right to vote.[17] In addition, citizens have the right to stand as political contestants and compete for votes, which includes the ability to identify and reach out to voters, hone political

15 "**Friends of Fidesz commit unprecedented privacy violations in Tisza app scandal**," Atlatszo, Nov. 2025.
16 See, for example, the cases of Hong Kong, the Philippines, Lebanon, Mexico, Turkey, and the US in "**Personal Data: Political Persuasion - How it works**" by Tactical Tech.
17 Articles 19 of the Universal Declaration of Human Rights (**UDHR**) and Article 25 of the International Covenant on Civil and Political Rights (**ICCPR**). **General Comment 34**, paragraphs 2, 4, and 7, UN Human Rights Committee (UNHRC). The UNHRC reviews implementation of the ICCPR and presents its interpretations of the treaty's provisions through its General Comments.

messages and respond to constituencies.[18] These rights are enshrined for all citizens regardless of race, gender, language, area of origin, political or other opinion, religion, or other status.[19]

However, the usage of sophisticated data-centric techniques like voter profiling or (micro)targeting may subvert these rights, as it provides campaigns and candidates with unprecedented abilities to influence specific voter groups while potentially excluding others, with LGBTQ+ voters, women, people with disabilities, migrants and diaspora, ethnic minorities, indigenous groups, and other politically marginalized groups being disproportionally affected. While parties have a right to understand and target their voters with tailored messages, this specific type of data use may create a risk of manipulation and prompt inequities in how different segments of the electorate receive political information and in their participation opportunities. These risks are further aggravated by emerging technologies like generative AI.

Snap Election faster than German DPAs: Microtargeting continues to influence voters

Political Microtargeting, Manipulation & Tracking / 21 February 2025

In March 2023, *noyb* filed complaints against several German political parties: During the 2021 elections, CDU, AfD, SPD, Bündnis 90/Die Grünen, Die Linke and the Ecological Democratic Party illegally used political microtargeting to attract voters. Now, almost two years later, we are just one day away from the next federal election. However, the competent Data Protection Authorities still haven't decided these cases – and political parties still use microtargeting. A well-know threat to democracy therefore continues.

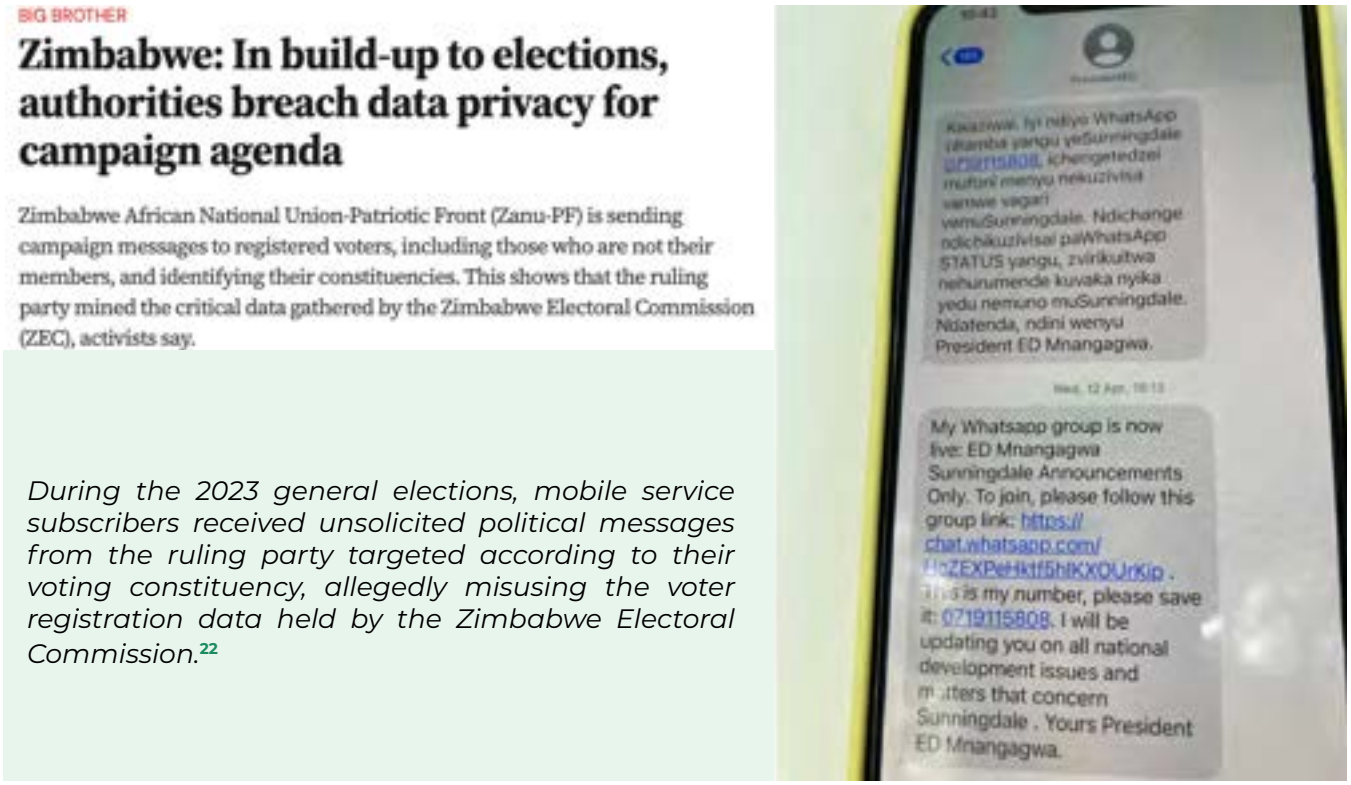
In the 2021 federal elections, German political parties used sensitive personal data, such as political views, to target internet users with personalised political ads. Austrian NGO noyb took action since political opinions are explicitly protected under Article 9 GDPR and should not have been used for advertising.[20]

- **The right to a level playing field:** Universal and equal suffrage, in addition to voting rights, includes the right to seek to be elected to public office without discrimination. Governments' obligations to ensure level playing fields for electoral contestants are derived from this norm.[21]

18 Article 25 of the **ICCPR**.
19 These obligations are founded in the freedom of expression provisions contained in the UDHR, the ICCPR, the UN Convention Against Corruption (UNCAC), the American Convention on Human Rights, the **African Union Convention on Preventing and Combating Corruption**, and the Organization for Security and Cooperation in Europe (OSCE)'s Copenhagen Document, among many others.
20 "Snap Election faster than German DPAs: Microtargeting continues to influence voters," Noyb, February 2025.
21 The UN Human Rights Committee provides guidance on this in its **General Comment 25** to the ICCPR.

However, this obligation may be undermined by inequality of resources, as better resourced campaigns have greater access to latest technology and data-centered campaigning practices. For instance, holding large volumes of personal data or the ability to profile and target voters at scale could amplify the inequality in resources and provide an election contestant with an outsized advantage.

Moreover, the unauthorized use of public data acquired by the state for campaign purposes is an abuse of state resources that can entrench incumbents. Similarly commercial and other personal data obtained through machinations of the state or political pressure is an abuse of power that creates unfair advantage.



BIG BROTHER

Zimbabwe: In build-up to elections, authorities breach data privacy for campaign agenda

Zimbabwe African National Union-Patriotic Front (Zanu-PF) is sending campaign messages to registered voters, including those who are not their members, and identifying their constituencies. This shows that the ruling party mined the critical data gathered by the Zimbabwe Electoral Commission (ZEC), activists say.

My Whatsapp group is now live: ED Mnangagwa Sunningdale Announcements Only. To join, please follow this group link: https://chat.whatsapp.com/ . is my number, please save it: 0719115808. I will be updating you on all national development issues and matters that concern Sunningdale . Yours President ED Mnangagwa.

During the 2023 general elections, mobile service subscribers received unsolicited political messages from the ruling party targeted according to their voting constituency, allegedly misusing the voter registration data held by the Zimbabwe Electoral Commission.[22]

- **Transparency and accountability in electoral actors and institutions:** Institutions are generally obligated to be transparent regarding electoral information so that voters can be informed about key processes and data sources can be held accountable.[23]

  However, voters may be unaware of how their information is being leveraged through consumer data brokers, social media platforms, and campaign apps. And even in places where the public awareness about privacy issues is higher, the lack of effective oversight over data matching and enrichment means voters have little to no control over how their personal information might be combined, processed, or shared once collected and entered into the campaign ecosystem.

  The challenge extends to campaign financing, where traditional reporting frameworks fail to adequately capture digital expenditures, creating accountability gaps in tracking data-driven operations.

22 "**Zimbabwe: In build-up to elections, authorities breach data privacy for campaign agenda**," The Africa Report, July 2023.

23 See, for example, General Comment 34, paragraphs 18 and 19, UNHRC.

In turn, technology companies intentionally obscure their data collection practices while creating barriers to external monitoring. Furthermore, platform policies on data use and algorithmic functions are often unclear, inconsistent, or deliberately obfuscated.

Particular threats in closed and closing contexts

While data protection and privacy has an impact on electoral integrity across contexts, there are particular impacts on closed and closing spaces. The use of personal data has been used by authoritarian and semi-authoritarian regimes to target individuals for censorship, surveillance, harassment, and even kidnapping and violence. In this context, insufficient data privacy protections - or blatant violation of such protections - can fuel broader political repression that can severely undermine the integrity of elections. This can be compounded by the growing trend of transnational repression, where diaspora and exiles are still tracked well beyond their borders via the collection and exchange of personal data, as well as other democracy activists.

CHAPTER 2:

OPEN DATA, ELECTION TRANSPARENCY AND DATA PROTECTION

Key Definitions[24]

Personal data (sometimes also referred to as "personally identifiable information") – It is any information that can be used to identify an individual. This includes obvious identifiers such as a person's name, address, email, or ID number, but also less obvious markers like mobile phone location data, IP addresses, cookie IDs, or even unique patterns in online behavior – essentially any information that could be used to single out an individual, either on its own or when combined with other information.

Personal data that has been rendered anonymous in such a way that the individual is no longer identifiable is not considered personal data, as long as such anonymisation is irreversible.[25]

The European Commission[26] provides the following examples of personal data:

- a name and surname
- a home address
- an email address
- an identification card number
- location data (for example the location data function on a mobile phone)
- an Internet Protocol (IP) address
- a cookie ID
- the advertising identifier of your phone
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Sensitive personal data – Are categories of personal data requiring higher protection due to their sensitivity (sometimes referred to as "special categories"), such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, sexual orientation, criminal records, biometric data, and genetic data. The categories vary by country based on local context, but commonly include those that may result in discrimination.

Biometric data – Data that includes **unique physical or behavioral information** used to identify an individual. It involves capturing and recording a person's biometric features for later comparisons to identify their identity. In many jurisdictions, biometric data is considered "sensitive" or a "special category" of data, as indicated above.

Data subject – A natural person whose personal data is being processed (this term is referenced in the definition of personal data as an identified or identifiable individual).

24 These terms may also be found in legal documents, but the actual legal definitions vary between jurisdictions.
25 European Commission, **What is personal data?**
26 European Commission, **What is personal data?**

Data processing – While sometimes defined more narrowly, it may also mean any operation or set of operations performed on personal data by automated or manual means, including collection, recording, organization, storage, adaptation, use, disclosure, restriction, erasure, or destruction. It can also include generation of data, as well as use of data to reveal other data.

Data controller – A natural or legal person, public or private, that decides the purposes and means of processing personal data (the "why" and "how"). In the electoral context, political parties, official candidates, or campaign headquarters and other organizations set up for campaigning purposes can be considered data controllers if and when they have the decision-making power with respect to personal data processing.[27] EMBs that collect and manage personal data for electoral administration may also be data controllers.

Data processor – A natural or legal person, public or private, that processes personal data on behalf of the data controller, typically limited to technical solutions and implementing the "methods and means" of processing. In the electoral context, public opinion research and voter analytics companies, as well as political consultants, campaigning tools and software vendors, or social media companies can be considered data processors, if and when they process personal data on behalf of controllers.[28]

Profiling – Any form of automated processing of personal data used to evaluate, analyze, or predict personal aspects concerning an individual's work performance, economic situation, health, preferences, interests, reliability, behavior, location, or movements. In the electoral context, profiling may entail automated processing of personal data – including with the use of AI – to analyze or predict certain personal aspects related to the data subject, such as that person's political opinions and his/her likelihood to vote for one party or another.[29]

Data protection authority (DPA) – An independent public body responsible for monitoring and enforcing compliance with data protection laws, investigating complaints, issuing guidance, and imposing sanctions on entities that violate data protection regulations.

DATA PROTECTION PRINCIPLES

While no single set of data protection norms has achieved global recognition, Privacy International outlines the following internationally recognized data protection principles[30] that can be derived from regional and international frameworks.[31] It is useful for election observers to know and understand these principles when monitoring data protection in elections, assessing practices and regulations, and providing recommendations.

27 See, for example, the definition under the Council of Europe's **Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns**, par. 3.
28 See, for example, the definition under the Council of Europe's Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, par. 3
29 See, for example, the definition under the Council of Europe's Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, par. 3.
30 Privacy International, "**The Keys to Data Protection**", 2018
31 See, for example "**A/HRC/39/29: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights**."

Lawfulness, Fairness, and Transparency: Personal data must be processed lawfully, fairly, and transparently. This means data collection must comply with legal requirements, respect individuals' reasonable expectations about how their information will be used, and avoid secret processing. Individuals must be clearly informed about what data about them is being collected, by whom, and for what purpose.

- For instance, when campaigning door-to-door, candidates or political parties (and their campaigners) must collect and use personal data in compliance with relevant legislation. They should be transparent about their data collection purposes and gather only the minimum necessary information. Campaigners should record only what voters voluntarily share about their own political views and preferences, without inquiring about other household members (especially children), tenants, or residents. They must not collect information about the household or possessions (such as vehicles or other items) to infer political preferences, as profiling entire households based on selective observations poses significant risks.[32]

Purpose Limitation: Data must be collected for specific, explicit, and legitimate purposes that are stated at the time of collection. The data cannot be used for purposes incompatible with the original stated purpose unless individuals consent or law permits it. The purpose must be defined precisely to avoid vague or undefined uses.

- For example, in the 2022 Hungarian elections the government repurposed the data it collected from people applying for state services to spread the ruling party's campaign message.[33] In this case, an incumbent utilizing voter data collected by relevant government bodies for other purposes in his/her political campaigning without notice or legal justification not only constitutes an abuse of administrative resources, but also violates data protection principles, such as purpose limitation or lawfulness, fairness, and transparency.

Data Minimization: Only personal data that is adequate, relevant, and necessary for the specified purpose should be collected and processed. Organizations processing personal data must use the least intrusive method to achieve their legitimate aims. Collecting extra data simply because it might be useful later or without considering necessity is unacceptable.

- For instance, in regard to voter registration, multiple international bodies and other relevant organizations recommend that only personal data which is required to establish eligibility to vote and nothing beyond that should be collected and included in the voter list.[34]

- The above guidance for political campaigners to gather only the minimum information necessary for further communication with voters when canvassing also illustrates the data minimization principle.

Accuracy: Personal data must be accurate, complete, and current. Organizations processing personal data should implement measures to ensure data quality and correct inaccuracies promptly. The "purpose test" involves assessing whether inaccurate or incomplete data could cause harm to individuals.

32 **Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns**, Council of Europe, par.4.1.11.

33 **Trapped in a Web The Exploitation of Personal Data in Hungary's 2022 Elections**, Human Rights Watch.

34 "Voter lists either should not include or should carefully protect personal data beyond that required to identify a voter and establish eligibility"– p. 59 of the **Election Observation Handbook, Sixth edition, ODIHR**; "The voters' register should not include personal data other than that which is required to establish eligibility to vote"– **Technology, Data, and Elections: A Checklist on the Electoral Cycle**, Privacy International.

- For instance, keeping the data on voter lists current – i.e. updating voter records if voters change their name (in case of marriage or divorce) or place of residence – is crucial so that individuals do not lose their right to vote.

Storage Limitation: Personal data should only be retained for as long as necessary to fulfill the purpose for which it was collected. Organizations processing personal data must establish retention schedules and securely delete data after the required period. Indefinite or blanket data retention violates privacy rights and increases security risks.

- While this principle dictates that election contestants or EMBs must not retain records for longer than necessary, it does not necessarily mean that political parties or candidates must delete collected data after the end of an electoral cycle, as they may find it necessary to communicate with voters for political purposes between elections. Similarly, an EMB or another relevant body may hold a permanent voter list so that eligible voters do not need to re-register for every election. However if a voter dies or otherwise becomes ineligible, then that voter information should be deleted and removed from storage under this principle.

Integrity and Confidentiality: Personal data must be protected by appropriate security safeguards against risks such as loss, unauthorized access, destruction, modification, or disclosure. Organizations processing personal data must implement appropriate technical and organizational measures to ensure data security throughout the processing lifecycle.

- Multiple instances of security breaches that resulted in unauthorized access to electronic voter databases and public leakage of voter information that took place around the world in the recent years would represent a violation of this principle, since they commonly resulted from the EMB (or other relevant bodies) failing to implement appropriate technical and organizational measures – such as encryption, access controls, regular security audits, and vulnerability monitoring.[35]


Online security lapses led to data of 40m UK voters being hacked, says ICO

Watchdog reprimands Electoral Commission for not being up to date with security updates before hack in August 2021

The data breach occurred in August 2021 but was not identified until October 2022. Photograph: Victoria Jones/PA

In 2021, the Election Commission of the United Kingdom suffered a data breach that resulted in the records of over 40 million voters allegedly ended up in the hands of Beijing, potentially exposing voters to the risk of foreign manipulation through the abuse of their data.[36]

35 See, for example, "**Breaches, Leaks and Hacks: The vulnerable life of voter data**,"Tactical Tech.
36 "**Online security lapses led to data of 40m UK voters being hacked, says ICO**," The Guardian, July 2024.

Accountability: Entities processing personal data must demonstrate compliance with all data protection principles and be held responsible for their actions. This includes facilitating individuals' rights, maintaining documentation of processing activities, and being subject to oversight by independent supervisory authorities with enforcement powers.

It is important to remember that in many places around the world no comprehensive national-level data protection frameworks have been enacted. Moreover, in places where these regulations do exist, they may have been outpaced by the rapid advancement of campaign technologies, meaning that even present legal frameworks often lack either strength or implementation.

*In 2019 EU elections, the European Data Protection Supervisor (EDPS) **investigated the European Parliament for passing the voter data to the US company NationBuilder**, known for its extensive data matching and targeting capabilities, as a part of voter mobilization efforts.*[37]

However, the absence or the shortcomings of national legislation do not take away the responsibility of electoral actors from the above mentioned data protection principles and election observers should still examine the electoral processes from a standpoint of privacy protections. Where regulations are absent or insufficient, the need for advocacy and reform becomes all the more compelling.

The Rights of Data Subjects

Individual rights constitute a fundamental element of data protection legislation, with those whose data is processed commonly termed data subjects (see Key Definitions above). In the electoral context, when assessing data subject rights, we generally mean the privacy rights of voters – whose personal information is processed by EMBs, political parties, candidates, and other electoral actors, including social media platforms and data brokers providing services for campaigns. These actors must fulfill voters' privacy rights, and voters should be able to enforce them through data protection authorities and courts.

37 "**European Parliament handed voter data to company linked to Donald Trump and Brexit**," Netzpolitik.org, November 2011.

As mentioned earlier, no globally recognized data protection framework exists, but a set of fundamental rights can be distilled from regional and international instruments.[38]

Among them:

- **the right to be informed** about data processing activities – for example, how voter registration data is collected and used;
- **the right to access one's personal data and obtain confirmation of its processing**;
- **rights to rectify inaccurate data** (such as correcting errors on voter lists), **block its processing** during disputes, and **request erasure** when there is no lawful basis for processing such data in the first place;
- **the right to object to processing** (for example, for direct marketing by political campaigns);
- **the right to data portability** in machine-readable formats;
- **specific rights regarding profiling and automated decision-making** – especially relevant for voter (micro)targeting practices – including the right to human intervention or to challenge a decision;
- **the right to effective remedies** through independent data protection authorities and courts, as well as **the right to compensation** for both material and non-material damages when rights are violated.

Together, these rights and their enforcement mechanisms establish a framework where voters maintain meaningful control over their personal information throughout the electoral cycle.

Election observers can use data protection principles and data subject rights as both an **evaluative framework** and an **advocacy tool** to assess whether electoral processes adequately protect citizen privacy and uphold democratic election principles.

OPEN DATA, ELECTION TRANSPARENCY, AND PRIVACY PRINCIPLES

Transparency is one of the key foundations for credible elections. Ensuring that key electoral data is available helps enhance the integrity of elections and hold the election institutions and stakeholders accountable. It also strengthens public confidence in the process and contributes to the acceptance of election outcomes. There are several **open data principles** that are critical for elections, such as making information available online in an accessible and analyzable format and at disaggregated levels, so that voters easily access election information, and electoral watchdogs and stakeholders – such as observer organizations, civic groups, political parties and media – can facilitate and use the data in assessments and analysis.

There is a misconception that respecting personal data protection and privacy in elections is at odds with open election data. In fact, governments, EMBs, technology companies and others have sometimes used bad faith data privacy arguments to restrict access to important

38 Privacy International, "**The Keys to Data Protection**", 2018

data and reduce electoral transparency. **However privacy and transparency principles can reinforce each other and both can be maximized in order to safeguard electoral integrity**. Key points to promote transparency while also supporting personal data protection in elections include:

Data protection protocols are part of open election data, and data privacy requires transparency and disclosure by key actors: Making data 'open' refers to sharing the data in ways that make data freely and easily used, distributed, and analyzed by the public, including making it freely available online. This includes information regarding how personal data is collected, secured, and processed by a range of stakeholders in elections, including the private sector. As part of key data protection principles,[39] the processing of personal data should be lawful and fair and done in a transparent manner. Transparency in political advertising is another example when open election data principles support privacy considerations, as opening data in this case helps shed light on such practices as microtargeting/profiling of voters.

Most open election data does not include personal data: Electoral data most often refers to aggregate or non-personally identifiable information, such as electoral boundaries, census data, campaign permits, technological procurement procedures, polling station lists or election results. There is no viable privacy argument for not making this kind of information available to the public. However there are some exceptions where key data sets may contain personal information. This includes items like **the voter lists, campaign finance disclosures, candidate details and election officials information**. In all cases these categories are particularly critical for voter information and the credibility and accountability of the process, and most still avoid sensitive details.

Observers can advocate for and analyze open data using privacy and protection principles: Observers can demonstrate their respect for personal data protection while also executing their mandates to scrutinize, assess, and synthesize election data. For instance, a key element of data protection is minimization, meaning that the processing of personal data should be adequate, relevant and limited to the necessity of the purpose for which it is being processed.

Election observers can ensure that unnecessary, extraneous, or sensitive data like ethnic or religious details are not disclosed, and only the information that is valuable to electoral integrity is processed and made available. In the instance of a voter lists verification exercise, this may mean access to only the key details needed in order to do a credible analysis and with flexibility for vulnerable groups. Observers should be sensitive to the risks that processing individual-level data may present to these populations. For instance, in some countries, publicly available voter lists exclude the information of exceptionally vulnerable citizens, such as victims of domestic violence or people in the witness protection program. In other cases, personally identifiable information in voter data like national ID numbers may be scrubbed from public voter lists. However, these are often made available to observation groups conducting an analysis of the rolls with the agreement to not to publicly disclose this data and to responsibly store it. Voter verification can also be credible with hashed data or only using the last four digits of the voter identification number and not the full number.

39 See **Open Election Data Initiative**.

Ultimately the legal framework should promote transparency around the rules and conditions for disclosure according to the type of data, and also guide the access and use of disclosed data by trusted actors such as citizen observers, parties or media. While data protection is essential, it should be used in a way that preserves transparency and enables meaningful oversight of electoral processes.[40]

40 A recent IFES comparative analysis of information related laws in elections highlights that when states adopt punitive information laws without transparency and accountability safeguards, they reproduce a similar pattern found in poorly regulated data ecosystems: opacity for authorities, asymmetry for political actors, and diminished agency for voters. Available at: **https://electionsandtech.org/research/digital-challenges-to-elections-2025.**

CHAPTER 3: CONSIDERATIONS AND CHALLENGES FOR CITIZEN ELECTION OBSERVERS AND DATA PROTECTION AND PRIVACY MONITORING

As data-centric practices and technologies in elections continue to proliferate, observers are increasingly called upon to examine them, including from the standpoint of data privacy and protection. And while they are accustomed to adjusting their methodologies to capture new and evolving issues, doing so within the framework of citizen election observation poses several notable challenges. Among them:

- **Bridging privacy considerations and electoral integrity:** As described above, data privacy rights address fundamental human rights concerns that reach well beyond the specific question of election integrity. Citizen election observers may face challenges in defining clear boundaries for their work and may be perceived as stepping outside of their mandate by other civil society actors. To maintain credibility, observers need to be able to demonstrate tangible links between personal data practices and the legitimacy of the electoral processes.
- **Interconnections with established observation areas:** The examination of electoral data protection cuts across multiple traditional observation domains, including political campaigning, misuse of government resources, digital election infrastructure and security threats, and the broader informational environment that encompasses social media ecosystems. Furthermore, data protection challenges and considerations will differ depending on the relevant actors, including electoral authorities, technology providers, and political parties and candidates. While this interconnectedness makes data protection monitoring relatively easy to integrate into existing monitoring approaches, not distinguishing it enough may also easily dilute the focus of observation in favor of other, more familiar areas.
- **Limited visibility of data practices:** The handling of personal data often occurs in digital spaces that lack transparency, including interactions among voters and political campaigns, relationships between campaigns or election management bodies (EMBs) and technology providers, commercial transactions involving third parties, and the administrative functions of EMBs. Since the processes for collecting, handling, and safeguarding this data are likely not readily accessible for examination, election observers need to develop indirect methods or apply a mix of approaches when assessing the effects of these practices on elections.
- **Technical capacity:** Likewise, monitoring personal data practices in elections may demand specialized expertise in relevant fields, including legal knowledge, technological understanding, digital analysis capabilities, or experience in Open Source Intelligence (OSINT), which could present obstacles for observation organizations with constrained resources or competing priorities. However, as discussed in detail below, there are many practical aspects of the electoral process that can be monitored by citizen observers that do not require specialized expertise. It is simply a different way of framing questions, and broadening the scale of stakeholders and processes within an observation.

- **Judgment calls:** Observers may find it challenging to distinguish between ethical campaign practices and data exploitation or to evaluate election data transparency needs vis-a-vis emergent data protection considerations. Assessing the impact of these issues on the electoral processes may require making judgement calls novel to citizen election observation frameworks.[41] However, any assessments should be rooted in – and can be defended by – international electoral integrity standards, which are discussed in more detail in Chapter I. In addition, simply revealing these practices without making a judgement or assessment can still be useful in enhancing transparency.

There are activists and advocates that are specifically focused on data privacy and protection, which goes well beyond elections. This includes safeguarding the ethical collection, use and storage of personal data in politics but also by digital platforms, commercial entities, in the health sector, and even by immigration or security actors. Election observers and other organizations working to safeguard privacy rights have distinct but complementary mandates when monitoring data protection in elections. Both groups aim to build transparency and accountability, provide recommendations to authorities, and advocate for reform. While other organizations may maintain a longer-term investigative and analytical perspective, election observers operate within a more defined temporal and methodological framework and are guided in their work by a set of strict principles. However observers should build linkages with these communities to ensure complimentary efforts and to learn from one another.

Election observers should primarily focus on concerns related to election integrity and assess observed data collection and processing practices by election contestants or electoral management bodies (EMBs) from this perspective. (This may also involve reviewing the role of technology platforms, election technology vendors, data brokers, or campaign consultants).

While the actual duration of monitoring may vary depending on the local context, observing data protection in elections is most insightful within the electoral cycle, in particular, when it involves real-time monitoring of ongoing campaigns. Additionally, election observers should focus their recommendations on improving data protection within electoral processes, regulations and laws.

In contrast, privacy watchdogs (or other civil society members concerned with data protection) take a broader approach. Their approach is not dictated by the electoral cycle and they may conduct in-depth investigations over extended timeframes, in between elections, or analyze data practices retrospectively to expose problematic technologies or avenues for data misuse not always detectable during election periods. For example, since the 2016 **Cambridge Analytica scandal**, many civil society organizations and academics have focused on researching the commercial industry of using personal data for political influences and its implications for democratic processes and societies.[42]

Ultimately, the relationship between civil society organizations concerned with privacy rights and elections observers is most beneficial when reciprocal. For instance, the former can further investigate issues flagged by observers, such as security incidents or problematic vendor relationships, while observer findings can highlight new areas of concern and vice-versa. They can also learn from each other. Citizen observers can gain greater insight into these issues while privacy rights groups can learn about how these issues play out in an electoral context. Both groups may find complementarity in their policy and advocacy efforts.

41 If available, observers may also engage the Data Protection Authority to assess some of their findings against the local data protection law.

42 For example, see case studies aggregated by the **Influence Industry Project** of Tactical Tech.

CHAPTER 4: FLOW OF PERSONAL DATA IN AN ELECTION CYCLE

Personal Data Use in Election Administration

The electoral process entails processing personal data at various stages of the election cycle. This information is critical to define and identify voter eligibility, ensure one person one vote, serve as the basis for redistricting, and generally to avoid fraud. However to effectively grant these rights to elect and be elected, EMBs are involved in the collection, processing, storage and use of massive personal data sets. Given the sensitivity of this data and its impact on electoral integrity, serious measures should be taken to safeguard these processes and the privacy rights of voters. Additionally, in some contexts, electoral data can be very closely integrated with other or broader public data systems.

Personal Data Use During Various Stages of Elections

Voter registration: The process of voter registration necessitates the collection of personal data used to register and verify eligible voters. This information can either be self-reported or automatically updated by state or governmental bodies. The state or governmental bodies in charge of the registry vary depending on the context but may include: The EMB (at the national and/or local level), the civil registry authorities, the Ministry of Interior, local authorities, and other specialized national agencies. The type of personal data collected at voter registration depends on the legal context but often includes: Name, family name, date of birth, address, gender, National ID number and in some cases party membership or voters' biometric data.

Use of biometrics in elections

Biometric data refers to **unique physical or behavioral information** used to identify an individual. It involves capturing and recording a person's biometric features for later comparisons to identify their identity. The use of biometric data is now common in daily life - for instance face or thumbprint recognition to log into your smartphone - and is also used in elections. It can help to create cleaner voter lists by capturing each voter's unique information at registration. The election administration then uses this data to identify duplicates by comparing each voter's unique biometric record. Additionally, the biometric data helps identify voters on election day and prevents voter impersonation or multiple voting. Biometric voter registration (BVR) is becoming an increasingly common practice.

Biometric data can include fingerprints, facial recognition, iris or retina scan or voice recognition - in elections, fingerprints and facial recognition are the most common. EMBs use specialized devices to capture the biometric features of voters. The device codes unique fingerprints 'patterns (also called minutiae) or facial measurements into encoded data. This data can then be stored, transferred and compared to other data sets to identify duplicates or to validate voters' identity on election day. Additionally, in a growing number of jurisdictions, national IDs include biometric data, thus making it available for processing also by EMBs.

THE FLOW OF VOTER BIOMETRIC DATA

Handling biometric election data involves several actors. While the EMB manages parts of the process directly, other elements rely on external vendors providing technology including the biometric devices as well as external servers for data storage and back-up during and between elections . The election administration must clearly define the role of external vendors in line with the country's jurisdiction requirements in terms of data protection and privacy. It should also ensure that the EMB maintains ownership and oversight over all aspects of the process. Additionally, given the sensitive nature of voters' biometric data, election administration should consider strong cybersecurity measures to ensure the integrity of the voter list and to deter and detect any intention to probe, temper or leak voters' data.

Transparency is essential when selecting the external vendors involved in the process. Election observers should be allowed to oversee all stages of adoption of these technologies. Election observers are encouraged to include the observation of use of biometrics within their data protection monitoring.

Candidate nomination and petitions: During the candidate nomination process, the election administration processes a set of personal data that extends beyond that required for voter registration. Potential candidates are typically required to provide personal data together with documentation that establishes their eligibility to run in an election in line with the legal requirements. Supporting documents may include criminal record, tax compliance or proof of citizenship. Additionally, in certain contexts, potential candidates are required to collect and provide several popular endorsements. In such cases, voters provide their names, ID numbers, signatures, and sometimes addresses, which the candidate collects and submits as part of the documents required for the nomination. This practice creates an additional layer of personal data processing involving endorsing voters' personal information which introduces additional risk to data protection.

Voter information and mobilization: A wide range of actors may engage in voter information and mobilization including civil society, EMBs, political parties and candidates. Effective voter outreach campaigns often target specific groups such as youth, first time voters and marginalized communities. Designing messages and outreach strategies that are relevant to these groups may require access to certain types of personal data.

Voter identification and voting on election day: Voter identification methods vary depending on the context and the type of technology used. These processes aim to verify voters' identity, prevent multiple voting, and ensure only eligible voters are allowed to vote. The methods for voter identification vary widely depending on the type of technology used. In cases where biometric data is used during voter registration, the same biometric system is often employed for voter identification on election day. In traditional systems, voter identification typically involves the use of printed voter lists at polling stations. These lists contain the names and details of eligible voters, which are checked against an official document – such as a national ID card or a voter card. Internet and other forms of online voting significantly increase data security risks, as they introduce more potential avenues for votes to be tracked to individuals and also additional vulnerabilities for interference.

Electoral dispute resolution: After the announcement of preliminary results, a dispute resolution process is opened to allow candidates and other stakeholders to challenge the integrity of the voting process or the election results. This process may require the collection of personal data and statements from individuals involved in, or witnesses to, the electoral process. Such information may be submitted as evidence to competent courts or electoral tribunals.

Election commission and polling officials recruitment: EMBs also process personal data of election officials of various levels who administer elections before and on election day. This may include their name, family name, date of birth, address, gender, national ID number. Depending on the recruitment and approval process, the data may include information about a commissioner's affiliation with a registered candidate or other public or civil society bodies nominating their representatives to the commissions.

Election observation: In many cases, election observers may be required to disclose the identity of their volunteers, and increasingly photographs of them, to obtain formal accreditation for observation or in order to provide formal testimony or documentation related to their observations.

National data centralization and comprehensive database

Many governments have been maximizing technological developments to improve the accuracy of public data and increase efficiencies between government agencies and services. For instance, in many places the voters list may be linked to the civil registry or public service databases in order to improve access and accuracy. However as governments are increasingly collecting and linking vast amounts of data about their populations, including through public service apps, smart city initiatives, service delivery upgrades, etc, it's important to understand how and where election-related personal data is stored and used throughout such systems, including what agencies have access to what information. This is not just for data security but also to prevent abuse. For instance, as part of the minimization principle, it does not make sense for security forces or public service ministers to have easy access to a citizens' voting history or party registration.

Risks and Vulnerabilities

The use of personal data by the election administration presents a number of risks. The systems put in place by the EMBs may contain vulnerabilities that could compromise the integrity of voters' data. These risks include:

- **Gaps in regulation or procurement agreements that fail to clearly define data ownership or other data security parameters between EMBs and vendors** – contracts between EMBs and private technology providers often lack explicit details regarding data ownership, access limitations, and security safeguards. Contractual disputes can tangibly affect electoral processes, potentially causing election postponements or withholding of critical databases.
- **Unjustified collection of excessive personal data** – EMBs may collect more personal information than is legally required and strictly necessary for voter identification and eligibility verification, violating the data minimization principle. This excessive data collection increases vulnerability to misuse and creates unnecessary risks when the purpose does not justify the extent of data gathered.
- **Weak security of systems employed for storage and use of personal data** – these systems may have inadequate access controls, insufficient monitoring for security breaches, and ineffective authorization procedures. Vulnerabilities in websites and infrastructure leave voter data exposed, with failures to regularly test security measures or implement adequate organizational and technical safeguards against unauthorized access, modification, or loss. The risks also extend to biometric data, including BVR kits being vulnerable to degradation and tech failure risks, as well as biometric data being stored together with other data (i.e in an open register accessible to the public or specific users).[43]
- **Unequal access of election stakeholders to personal data** – while political parties have legitimate interests in accessing voter list data, laws often fail to clearly stipulate who can access such data and for what specific purposes. Some countries maintain both full registers (restricted access) and open registers (purchasable by anyone), creating disparities where better-resourced actors gain advantages through more

43 **https://privacyinternational.org/advocacy/5447/elections-technology-our-recommendations-1-general-recommendations-bvr-evid-and**

sophisticated data access, while inadequate restrictions enable unfettered access that can facilitate voter manipulation.

- **Risks of data breaches, leaks and hacks by malign actors** – electoral databases face significant threats from hostile cyberattacks and security failures. Major breaches have exposed millions of voters' personal and sensitive data (e.g., biometrics), including instances where EMBs failed basic security tests, had vulnerabilities in their systems, or lacked adequate monitoring for suspicious activity, enabling unauthorized access to passport information, tax identification numbers, addresses, and other sensitive details that can facilitate identity fraud.
- **Data retention beyond electoral cycles** – EMB's should ensure that personal voter data is not stored longer than necessary for its original purpose. Indefinite retention increases security risks, creates opportunities for data misuse for unintended purposes, and represents an ongoing infringement on privacy rights, particularly when clear retention schedules and deletion procedures are absent. Additionally, the retention of personal data beyond elections should be explicitly specified in the EMB's agreement with external vendors.

PERSONAL DATA USE IN ELECTION CAMPAIGNING

It is now common for political parties to maintain digitized databases of their members, supporters, and regular voters and utilize sophisticated data-centered technologies for election campaigning and, increasingly, for in-between election outreach. They are assisted by specialized companies and consultants, tech platforms, and data brokers.[44]

Ethical campaigning: Political parties and candidates have a legitimate right to compete for votes by engaging with the electorate, including via data-centric campaigning practices. From a privacy standpoint, a model campaign collects and uses voter data only for clear purposes like sharing its platform, recruiting members, inviting voters to events, or encouraging them to vote, and it should openly inform voters where it got their information, who it's sharing it with, and give the voter a choice to say no or have their data deleted. The campaign should be open about whether it is using data brokers or targeting companies, and it shouldn't manipulate voter data or use it in hidden ways that undermine fair elections. A problem is that parties or candidates that choose to protect voter privacy this way are at a disadvantage against competitors who use aggressive and non-transparent data collection, profiling or (micro)targeting techniques to influence voters. This means that unless data protection laws require all parties to follow the same rules, individual campaigns have little reason to voluntarily protect voter privacy; doing so would make them less competitive against opponents who choose to exploit voters' personal data without limits.

Alongside commonly used methods, such as online political advertising, phone banking, or e-mail marketing, a cohort of more sophisticated techniques have been developed and deployed, including (micro)targeting, location tracking, digital listening and sentiment analysis, psychometric profiling, and others.[45]

44 For instance, Tactical Tech has identified and compiled a **database** of over 500 commercial vendors offering data-centered campaign technologies and services to political campaigns.

45 Here are some **learning resources** on various technologies used in political campaigns by Tactical Tech.

Examples of data-centered campaign techniques & methods:

- *(Micro)targeting* – Targeting individual voters with personalized messages – on the basis of provided or inferred preferences – through online services such as social media platforms and instant messaging services.
- *Psychometric profiling* –The process by which one's observed or self-reported actions are used to infer their personality traits.
- *Geotargeting* – Using location information to target a person with particular ads or messages.
  - *Geofencing* — Creating a virtual perimeter around a point of interest to promote a message only to individuals inside that area.[46]
- *A/B testing* — Sometimes called split testing, compares two or more variants of an advertisement or message to determine which one performs best.
- *Robocalling* – Auto-dialing a list of phone numbers in order to deliver a prerecorded message or even conduct a live call (when more advanced technology is available)l
- *Digital listening and Sentiment analysis* – Digital listening involves monitoring and analyzing what someone does or says on social media platforms, including both the behavior and the content. While sentiment analysis measures whether content shows a positive or negative attitude.[47]
- *Online cookies and other trackers* –
  - *First-party cookies* are needed to improve user experience with the website. Third-party cookies are often used to track an individual across the web and cross-reference information about them.
  - *Other tracking services,* such as tracking pixels, beacons, keyloggers, etc.[48]

46 For example, in the 2015 elections in Guyana, the US-based tech company El Toro mapped users' IP addresses to their home addresses, enabling the campaign of David Granger to send personalized ads to single households and devices, even when they left their homes or offices. (For more on Geofencing, see "**Personal Data: Political Persuasion: Inside the Influence Industry – How it works**" by Tactical Tech).

47 For example, in the 2014 elections in India, Germin8 Social Intelligence service provider published analysis of social conversations in the run-up to the 2014 elections. The results showed that the Bharatiya Janata Party (BJP) had a more positive message focusing on hope, whereas the Aam Aadmi Party had a critical approach that focused on issues such as corruption. (For more on Sentiment analysis, see "**Personal Data: Political Persuasion: Inside the Influence Industry – How it works**" by Tactical Tech).

48 **Tracking pixels** (also known as web beacons, pixel tags, or spy pixels) are a technology used to monitor user behavior online and in emails. They are typically a tiny, transparent 1x1 pixel image file embedded in the HTML code of a webpage or email. When the user's browser or email client loads the image from the sender's server, the server logs data, indicating that the content has been viewed. They can collect the user's IP address and location, the device and operating system used, and whether the email was opened. Meanwhile **keyloggers** are stealthy software or hardware tools that secretly record keystrokes typed by users, capturing sensitive data like passwords, credit card numbers, and private messages, often delivered via malware, phishing, or Trojans to steal information for fraud, unauthorized access, and corporate espionage, requiring strong antivirus and security awareness to detect and prevent.

Data Types and Sources

Where do parties and candidates get data used for election campaigning? A variety of sources and data collection methods exist, and often parties and campaigns may combine multiple datasets.

Voter registration records: Compiled for the purpose of administering elections and increasingly digitized, voter lists typically contain information about all citizens eligible to vote, including one's name, date of birth, address, and gender. Often, the lists are provided to political parties or candidates for campaigning purposes on a national or local level.[49]

Political parties and candidates: Parties, their elected representatives, and candidates collect troves of data during their communication with voters offline and online. Depending on the methods used, they may be assisted by campaigning tech providers, specialized consultants, or social media platforms (see the list of campaigning tools below).

The data collected about voters may contain information similar to that found in the voter list, but may also extend to encompass a variety of other aspects, including one's likelihood to vote, additional and updated contact information, economic status, issue positions, or such sensitive data as a voter's race, health status, political or religious affiliation, and other. This data is used to build, update, and enrich records held by a contestant or campaign HQ.

It may also feed into a larger database held by the candidate's party on a local, regional, or national level. Based on applicable data protection laws and parties' operations, such databases may be then reused for future campaigning, including by other candidates, used by party's elected representatives, traded to or sold to like-minded groups, etc. Notably, the voters may not always be aware of how the data they provide during the campaign is utilized beyond the current electoral cycle.

In addition to data about regular voters, political parties usually maintain member lists, which they may be required to share with the government. These lists could contain information about one's length of membership in the party, positions held, donation history, and even voting records. Parties also draw on their member lists for election campaigning – for example, for soliciting donations or recruiting volunteers.

Data brokers or campaign technology vendors: Parties and candidates may purchase data about their potential voters from commercial data brokers or providers of campaign technology, such as customer (or constituent) relationship management (CRM) software. Offering a combination of various services, such companies may themselves collect data and profile voters for their clients matching publicly available records with consumer and other information (i.e., financial records, subscription data, data from social media profiles, smartphone location data, IP addresses, streaming device viewing behavior through automated content recognition technology, and other).

49 For example, voter lists are made available to political parties, candidates, and/or members of Parliament in the UK, Australia, Canada, the US. An open, or "edited," register also exists in the UK, which essentially contains the same information and is **openly sold**. However, voters can opt-out of being included on the Open register.

For example, US-based CRM software provider NationBuilder offers users targeting and data matching functions, including linking contact data like e-mail addresses with respective persons' social media profiles.

Social media platforms: While not necessarily sharing data of their users with election campaigns, social media platforms offer political parties and candidates vast capabilities for targeting potential voters with tailored political messages via online advertising capabilities. For instance, Facebook's Custom Audience feature allows uploading lists of targeted persons to the platform for matching with their user profiles.[50] The extent of matching and targeting services offered by the platforms may differ based on the applicable data protection and digital political advertising regulations.[51] However, despite increased public pressure and regulations demanding greater transparency, the exact methods through which voters are targeted on social media platforms remain a blackbox, even to the political parties or other election contestants who are paying for these services.

The European Union has established a comprehensive regulatory framework for political advertising through two key pieces of legislation: the **Digital Services Act** (DSA) and the 2024/900 Regulation on Transparency and Targeting of Political Advertising (TTPA). The DSA, which entered into force in October 2022, establishes baseline transparency requirements for online advertising, requiring **Very Large Online Platforms** and **Very Large Online Search Engines** to create repositories containing information about advertisements, including who paid for them and targeting criteria. The DSA also **prohibits advertisements** based on profiling using special categories of personal data.

Building on the DSA framework, Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising entered into force on 9 April 2024, with the majority of its provisions becoming applicable on 10 October 2025. The TTPA requires that each political advertisement include a transparency label and notice identifying it as political advertising, disclosing **the sponsor, amounts paid, and any targeting techniques used**. Under the TTPA, targeting or ad delivery of political advertising online is only permitted under strict conditions: data must be collected directly from the data subject, explicit and separate consent is required, special categories of personal data cannot be used for profiling, and personal data of individuals at least one year under voting age cannot be used. To prevent foreign interference, the regulation bans third country sponsors from providing advertising services three months before an election or referendum.

50 In recent years, providers of targeted online political ads have come under fire for using so-called sensitive categories of users' personal data, with such platforms as Facebook and Instagram consequently **limiting their own political targeting options**.

51 Additionally, the use of Facebook's Custom Audience feature has been previously significantly **curbed by the EU privacy regulations**, notably the General Data Protection Regulation (**GDPR**).

Notably, in response to the TTPA, Meta and Google **withdrew political advertising services from the EU** as of October 2025.

Third parties: In some contexts, political parties or candidates may also use the data collected by various interest groups, issue-based initiatives, etc., for election campaigning. These data sharing practices may be a strong organizing tactic for like-minded political groups. At the same time, they are not always transparent to the voters whose personal data is being used and can be scrutinized by election observers from this point of view.

Data Scraping and Hybrid Profiles

Complementary IFES-led **research on generative AI (genAI) in political communication highlights** that genAI dramatically lowers the barriers to creating "synthetic personas", or fake accounts that convincingly mimic real voters. These accounts often blend scraped personal data (e.g., names, photos, demographic details) with AI-generated behavior. While the synthetic content itself may not contain protected personal data, these tactics depend on initial data extraction and repurposing that can violate data protection norms related to lawful processing, transparency, and purpose limitation. For observers, this means that monitoring coordinated inauthentic behavior may also reveal upstream data protection harms.

Campaign Data Collection Tools and Methods

Political parties and candidates may collect voters' data during offline campaigning events, such as political rallies or canvassing of voters using a mixture of paper records and digital instruments, such as mobile canvassing apps or CRM software.

In turn, many digital tools commonly used to communicate with voters are also utilized to collect data about users and feed it back into candidate or political party's databases. These tools are more readily "observable" due to their public nature. The extent and transparency of their data collection functionality may differ from place to place based on local data protection regulations. For example:

Offline data collection during canvassing and other campaign activities and events – Political parties and candidates typically collect voter data during offline events and activities. With the proliferation of data-centric campaigning technology, campaigners are more than likely to be assisted in their field work by various tech tools, either digitizing data collected on paper shortly afterwards or directly inputting it into a centralized database via mobile apps, CRM systems, etc.

Feedback or sign up forms on websites and social media – While these instruments allow subscribers to receive direct communication from the party or candidate of interest or pledge their support, they typically collect personal information about subscribers that can be used for further campaigning.

Online donations – When soliciting donations from citizens, parties and candidates may be obligated by law to report certain information about donors to overseeing bodies. In addition, while credit card information is typically securely transmitted to payment processors, it may

also be stored by recipients if donors opt for recurring contributions.

Website audience tracking and analysis tools – These tools differ in their sophistication but may allow website administrators to collect quite granular information about visitors that could enhance the database of the party or candidate. Users may or may not be alerted about the use of these instruments based on the local data protection regulations or website owner's data protection policies.

Social media – Creators and administrators of social media profiles/pages/channels/groups may gather user profile and engagement data (like, follow, share) and pass it to the respective candidate or party for further use in campaigning activities. Social media is also increasingly used for digital listening (see the section on data-centered campaigning methods).

Online registration forms – Typically, these forms ask for personal data including person's name and contact information in order to engage them in a campaign activity or event; however, candidates or parties rarely limit their communication with the voter to just the information concerning an activity he/she has signed up to for, which may not always be apparent to the latter.

E-mail marketing software – In addition to requiring user contact information, many automated e-mail solutions also collect a variety of other data about recipients, such as geographic location (IP addresses), type of devices used, frequency of opening received messages, and other engagement metrics. This data may then be used for further analysis and optimizing communication as well as for enriching a party/candidate's databases.

Online petitions – While created for advocating around issues or policies, petition platforms may display some of signees' data (such as name and location) publicly or share it in part or in full with the petition's creator. This prompts parties and candidates to use petitions as effective data collection tools.

Mobile campaign apps – Mobile apps provide an easy way to communicate with the candidate, party, and other supporters within a specialized environment and can capture various types of data about users that are fed into a campaign database.

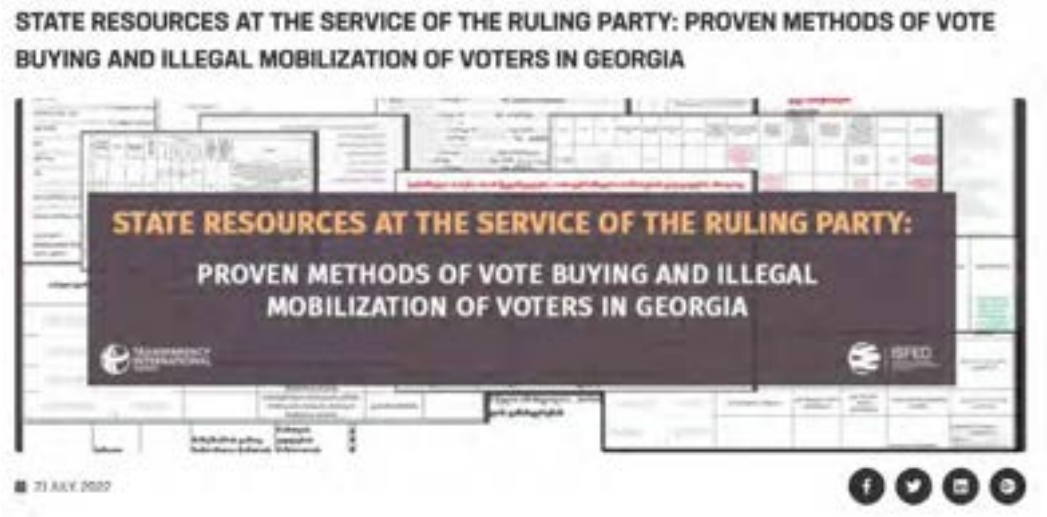
Chat bots – Chat bots are increasingly easy to integrate on social media or websites. The platform providing chatbot functionality may share data of users that interact with the chatbot with its creators.[52]

Risks and Vulnerabilities

As discussed above, political parties and candidates have the right to reach out to and communicate with their voters. In other words, not all data-centered campaigning practices are necessarily problematic – some are legitimate ways of delivering political messages to citizens. However, the proliferation of data-centered campaigning methods creates a number of risks for election integrity. Among them:

52 For example, Telegram - a popular messaging platform - allows users to create their own chatbots. However, Telegram Privacy Policy states that most bots developers are completely independent of Telegram and **should ask user permission before accessing or sharing their data**.

- **Data matching, inference, and profiling of voters at scale:** The scale on which data about voters gets collected, cross-referenced, and matched allows parties and candidates to profile voters with increasing accuracy and granularity, including enriching these profiles with information inferred based on already available records. For instance, the Council of Europe specifically warns that sensitive "information on political opinions might be revealed or inferred through predictive analytical and profiling tools from a range of other sources of information[53]." This raises a number of concerns as discussed in the "Personal data protection as an election integrity issue" section, in particular, the manipulation and transparency risks posed by (micro)targeting and risk of voter discrimination, including voter disenfranchisement or suppression. Notably, while local data protection laws may limit the extent to which voters could be profiled and targeted using such practices,[54] technological developments have outpaced regulation in many places.
- **Abuse of incumbency and abuse of state resources:** The increased digitization of public services by the governments means accumulating an ever growing volume of digitized citizen data, including sensitive categories of data, data of vulnerable groups, etc. Weak safeguards against unauthorized access to such data by incumbents prompts abuse of administrative resources and may provide an outsized advantage in an election campaign or facilitate such practices as voter coercion or vote-buying.



In the 2022 elections, Georgia's ruling party abused the data held by the law enforcement agencies to illegally incentivise citizens to vote, offering specific persons the cancellation of probation, early release from the penitentiary institutions, restoration of suspended driving rights, etc.[55]

53 See **the CoE Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns**, par. 4.2.2.

54 For instance, the Spanish Data Protection Agency (AEPD) **prohibits the processing of personal data from which political opinions can be inferred**, except for those that have been freely expressed by individuals in the exercise of their rights to ideological freedom and freedom of expression. This means that technologies like mass data processing or AI cannot be used to infer a person's political ideology from other personal data. In France, the regulators **prohibited parties and candidates in the 2017 elections from enriching their voter databases with information publicly available about these voters on social networks**, since the latter could not object to being profiled in such a manner.

55 "**State resources at the service of the ruling party: Proven methods of vote buying and illegal mobilization of voters in Georgia**,"Transparency International Georgia and the International Society for Fair Elections and Democracy, July 2022.

- **Data security:** Similarly to the use of digitized voter data in election administration, data-centered campaigning increases the risk of data breaches, leaks, and hacks by malign actors. Cases of illicitly obtained data being published or sold online are increasingly common and may prompt abuse, including in the context of election campaigning.
- **Data retention and campaigning outside of the official campaign period:** As noted, parties can retain voters' personal data for communicating with the voters in between elections. However, aided by available data-centric technology, this effectively results in the emergence of a permanent campaigning cycle, with political actors continuing to collect and utilize voter data outside of the periods typically scrutinized by election observers and EMBs.
- **Data sharing between parties/candidates and third parties:** Data sharing between political parties or candidates and data brokers, campaign technology vendors, or issue groups and other non-partisan organizations often lacks sufficient transparency, making it difficult for observers to scrutinize these practices and for voters to understand how their data is being handled. Data sharing also increases the risks of unauthorized access or disclosure if adequate security measures are not in place. Political parties may also fail to assess whether third parties comply with data protection laws or whether they obtained data lawfully before using it, potentially exposing voters to unlawful processing.

CHAPTER 5: PLANNING AN ELECTION OBSERVATION EFFORT

Planning an election observation effort requires several stages including conducting a risk assessment, defining the scope and focus of observation, choosing the right monitoring tools, and evaluating the right moment and format to publish the findings. As discussed above, data privacy and protection intersect with numerous human rights issues, making it challenging for observers to maintain a focused scope and make a distinction between broader data protection concerns and issues that could impact on the electoral process. Moreover, personal data protection naturally overlaps with conventional areas of scrutiny such as campaign activities, electoral technology and security measures, and the broader information landscape including social media platforms.

RISK ASSESSMENT

Preliminary risk assessment of their electoral and political environment may help observers determine the relevance of data protection monitoring in their context vis-a-vis potential threats to electoral integrity. It can also provide information that would help monitors decide whether data protection warrants a standalone focus or should be integrated throughout other elements of their methodology.

What to take into account in a risk assessment differs in every context, and in the context of monitoring data-driven practices and technologies the following aspects are a guide to the minimum and/or necessary unique aspects to take into account:

Legal environment

- Is there a national personal data protection law? Are there other relevant regulations that could impact how personal data is used in elections (for example, relevant personal data disclosure or protection requirements in the election law, freedom of information, cybersecurity, or online media legislation)?
    - Are there any exemptions for political parties or public bodies?
    - Have data protection laws been unevenly or inconsistently applied, especially in the electoral context?
- Do data protection laws come with appropriate oversight and enforcement mechanisms? (What are they?)
- Do campaign finance laws sufficiently regulate and promote transparency in online political advertising? What type of disclosures about social media advertising are required of election contestants?
- Are there any specifics related to data use by the EMB, including restrictions on publications, cybersecurity requirements, etc.?
- Is there complementarity between measures aimed at increasing electoral transparency and data privacy laws? Or is there confusion or vagueness in mandate and principle?

- What rights do observers have? Can they access necessary information freely?

Election technology

- Do any of the election technologies utilize personal data? What is it and at what stage of the electoral cycle is it deployed?
- What type of voter data is being collected and processed by this technology?
- Is any biometric data being used?
- Does the legal framework outline the chain of custody for personal information collected along the election cycle?
- Are there clear regulations or procurement agreements for the role and scope of the external vendors dealing with personal data? Does the EMB maintain ownership of the data?
- How is data stored during elections?
- What are the data security protocols in place to protect the data?
- How is data stored in between elections? Is there a clear deletion protocol?

Campaign practices

- Are social media platforms or direct messaging apps a major source of political news and/or an important place for political discussions for voters? If so, which platforms are most common? Do those platforms have any regulations or policies regarding microtargeting, or political ad transparency?
- How widespread is the use of social media marketing, direct marketing, or other data-centric commercial practices by businesses? (May indicate possible "spillover" into political campaigning).
- How common and developed is digital election campaigning?
    - What campaigning practices that utilize personal data are already known to be used by election contestants?
        - For example, (micro)targeting and profiling with the use of sophisticated tools?
    - What digital tools are being used by election contestants to communicate with and collect data about voters? How important are they for campaigning?
- To what extent do political candidates and political parties collect and store voter information during offline events and through telephone calls? Are they required to disclose any details about their voter outreach and information storage?

Essential background

- What is the overall political and electoral context? (For example, what are the general expectations regarding the quality of the electoral process?)
- Is there a history of past data protection violations or security incidents by election contestants or EMBs that can help observers identify potential high-risk practices?
  - For example, is there a risk of personal data exploitation by an incumbent, either to mobilize or intimidate voters?
  - Is there a suspected illicit data flow between election contestants and public officials, civic groups, private companies, and/or EMBs?
  - Is there a history of prominent data leaks, hacks, and breaches or other security concerns?
- What other context-specific concerns may impact the risks related to data protection and election integrity? (For example, overall privacy culture and the level of public awareness about data protection issues in elections).
- Are there any emergent trends or issues that may affect data protection in elections? (For example, arrival of new companies or consultants specializing in data-centered campaigning or emergence of new technology).
- Is anyone already working on these issues and what are they focusing on specifically?

DETERMINING SCOPE AND FOCUS OF MONITORING

Observers should set monitoring objectives that are clear, realistic and narrow in scope. They should be derived from the preliminary assessment of the risks to election integrity related to data protection.[56]

The following set of questions could be helpful to determine and narrow the scope of observation.

<u>What</u> will be monitored?

- Do observers want to focus on the use of personal data by election contestants or EMBs? Or both?
- What data practices and at what stages of the electoral cycle should be monitored? (E.g., the use of personal data during voter registration, voter mobilization, election campaigning, voting, etc.). Are there specific risk areas that need to be scrutinized closely?

<u>Who</u> will be monitored?

- If election contestants are a focus – should all or a set of candidates/parties be monitored? How will the selection be made?

56 See an example of an international election observation mission **scrutinizing the use of technologies and data in the 2022 Kenyan elections**.

Note: It is important to remember that with the addition of each new "target," the list of associated methods, platforms, and tools that would need to be covered by monitoring may grow exponentially.[57] Choices need to be made with available resources and existing limitations in mind (see sections below).

- If EMBs are a focus, will monitoring need to be conducted on the national, regional, local level or some combination of those?
- Are any private firms commissioned by the EMB or hired by the election candidates and also need to be monitored?

<u>Where</u> will it be monitored?

- What methods, platforms, and tools are used for data collection and processing by the chosen actor(s) during the respective stage of the electoral process? Which are most frequently used? Are there any vulnerabilities or other concerns that call for increased scrutiny?
  - Will observers need to focus on the online data-centered practices or also monitor offline data collection?[58]
  - For online data collection and processing, which websites, social media, and other instruments need to be monitored?

<u>When</u> will it be monitored?

- When does the monitoring start and how long does it need to last? Should it extend beyond the electoral cycle?

  Note that many election websites and other digital tools, especially the ones used for campaigning, are short-lived and may be taken offline right after election day.

<u>How</u> will observers collect and analyze data?

- How will observers preserve such evidence of their findings as webpages, websites, and other digital tools?
- What questions will they ask about these digital instruments or what criteria will they assess them against?

57 For example, see this case study of the 2024 elections in India by Tactical Tech for the extensive list of non-affiliated actors involved in election campaigning: "**Regulating Diffuse Actors in the 2024 Indian Elections**."

58 Given the extent of available tech tools, it is highly likely that even at offline data collection activities - for example, during canvassing or the voter registration drive - the data would immediately get processed with the help of some digital means (i.e., input into an electronic database) and may feed into existing online tools.

Retrieving and archiving information from websites:

When monitoring data protection in elections, observers may want to preserve webpages, websites, and other digital tools they come across as evidence to back up their findings. There are a variety of ways to do that – from making screenshots of relevant pages to using services that automatically archive prior versions of websites. When taking screenshots, monitors should capture entire webpages rather than just isolated messages or images, including the URL bar, timestamp, and surrounding context. They should also consider combining manual screenshots with third-party archiving services like the Internet Archive's Wayback Machine and Archive.today to create multiple backups if one method fails or the original content is removed. More information about retrieving and archiving information from websites may be found in the **Exposing the Invisible kit**.

Case study: The use of voter personal data in the 2019 Ukrainian parliamentary elections

Ukrainian citizen election watchdog OPORA and NGO Digital Security Lab-Ukraine, in partnership with Tactical Tech (Germany), examined how the most successful political parties in Ukraine's 2019 Parliamentary elections leveraged personal voter data. Authored by the Prague Civil Society Fellow Tetyana Bohdanova, the **2020 report** documented a wide range of data collection mechanisms and targeted digital campaigning methods being used by major political entities against the backdrop of legal loopholes in campaign finance regulations, shortcomings of digital platforms, cybersecurity lapses, and ambiguities in the country's data protection regulations.

SELECTING MONITORING METHODS AND TOOLS

When embarking on monitoring the use of personal voter data in elections, observers should formulate a series of questions that will guide them in their observation efforts and analysis. Below is a list of potential monitoring questions.[59] The actual questions selected should be based on the monitoring objectives derived from the preliminary risks assessment.

Model Questions when Monitoring Data Protection in the Use of Technology in Election Administration

- What type of technology is used when it comes to capturing, storing and using voters' data?
- How is this technology procured? Is the process transparent allowing scrutiny from election observers?
- Where is the data stored?

59 For more questions and recommendations to consider when monitoring the use of personal data in elections see Privacy International's Technology, Data, and Elections: A Checklist on the Electoral Cycle, NDI's Monitoring Electoral Electronic Technologies: A Model Checklist and Recommendations for the Adoption of Electronic Electoral Technologies.

- What measures are in place to clarify the role of vendors while ensuring the EMB maintains overall ownership?
- Who has access to that data within the EMB? Who has access to the data outside of the EMB? For instance, is it shared with other government entities, and is there a protocol in place for what parts and how it's shared?
- What measures are in place to protect the data security of this sensitive information?
- How robust are the data security measures in place protecting voters' data?

In case biometric systems are used for voter registration and identification:

- How is voter information stored? Is it stored on the registration device directly? Is it also transmitted onto a cloud-based server? How is the data protected at the machine level, during transmission and the central level?
- How is voter information transmitted to a central aggregation center?
- What security measures are in place to ensure that the voter information is not compromised?
- Who has access to biometric data? This includes both within the EMB but as well as outside of (for instance, tech vendors, and whether biometric data is shared with other government entities)? If shared with other government entities, what data practices do they follow?

Model Questions when Monitoring the Use of Data in Election Campaigning

- Is there a national data protection law? Does it establish an independent data protection authority (DPA)?
- If there is a national data protection law in place, does it apply to political parties or candidates?
    - Is there special guidance of using personal data in the electoral process issued by the DPA or another relevant body?
- Do political election contestants (parties, candidates) have data protection policies that are accessible to the public?
- How do election contestants collect and use (process) voters' personal data? What types of data do they collect? Do they disclose it?
    - Is there any indication they might be collecting sensitive categories of data?
    - Do they request consent of the voters (data subjects) for processing their personal data?
- Do their practices comply with the data protection law and other applicable regulations?

- Are there any contradictions between election contestants' stated data protection policies and their actual practices? Between their actual practices and legal obligations under the data protection law or other relevant regulations?
- Are the election contestants using the services of any data brokers, campaign technology vendors, or consultants?
    - Is voter data held by the election contestants being shared with third parties?
- What security measures have election contestants implemented to prevent unauthorised access of personal data? Do they seem robust enough / are they consistently implemented?
- Have there been any instances of voters being contacted by political campaigns and not knowing how they got their information?
- Do parties or candidates that are connected to national or local government appear to have the same level of voter information as their political competitors?
- Have observers witnessed the government engaging in any campaign activities, and if so, did this use voters' data in any way?

Monitoring Methods and Tools

The list below includes monitoring methods familiar to citizen election observers as well as those more common to researchers or data protection specialists. It is by no means exhaustive.

The methods selection will depend on the objectives and scope of the monitoring, as well as on the available skills and resources (see the section below). Most of them can be applied to both monitoring the data collection practices of EMBs and election contestants. It is important to consider the methods alongside their limitations.

- **Desk review of pre-existing research, media articles, and other monitoring reports** - This can serve as an invaluable resource for election observers who are frequently constrained in their resources and capacity. In particular, it may provide observers with essential background and analysis of the legal and technical environment, documentation of specific data-driven campaign methods and their historical use, patterns of data flows between political actors, data brokers, vendors and EMBs that may not be visible during election periods, and information on past security vulnerabilities and data protection violations that highlight compliance gaps and high-risk practices. As discussed previously, this method could also be used during the pre-election risk assessment.
- **Legal framework analysis** – When monitoring the use of voters' personal data, observers should add the examination of specific laws governing data protection and their application to the electoral process, as well as review of elections-related regulations, e.g., on campaign finance or the use of digital technologies, through the lens of data protection. It is important to not just consider legal texts, but also their practical implementation by election management bodies, political parties and candidates, and other data controllers, as well as the work of regulatory bodies, such as data protection authorities. As mentioned above, the review may also bring up such problems as inconsistencies between data protection and electoral laws or

contradictions between election transparency considerations and data protection requirements. As with any other legal analysis, any assessments and recommendations should be rooted in the international electoral integrity standards.

- **Direct observation of data processing practices**
  - **Election contestants** – This method involves election observers systematically monitoring how political parties and candidates collect, use, store, and share voters' personal data during campaigning and voter outreach activities. As discussed above, observers may examine various campaign data collection and processing methods including offline canvassing or targeted digital advertising, monitor the use of commercial data brokers, campaigns and technology vendors or consultants, etc. (For example, unique email addresses may be used to subscribe for political communication of parties or candidates or register for campaign events, to more easily trace the "journey" of this piece of data once it enters the digital campaign ecosystem). While election contestants' data practices could be assessed against local data protection regulations, specific guidance issued by the DPA, their own data protection policies (if present), as well as general data protection principles (see Chapter 2), the ultimate goal for observers is to determine whether their findings could have an impact on election integrity (i.e., based on principles discussed in Chapter 1).
    - **Review of campaign technology vendor documentation** – Vendor contracts are rarely available to observers, as the former typically claim proprietary protection over their methods and algorithms. However, commonly available tools and platforms typically have publicly accessible documentation that could help observers understand and assess their handling of users' personal data. Such documents may include: Terms of Service, Privacy Policies, Data Protection Notices (as required under GDPR), Political Ad Policies and Ad Transparency Libraries (as required under the EU Digital Services Act), API documentation, voluntary Platform Commitments related to elections, and Help Center Information explaining how advertising, profiling, or targeting services work.
    - **Review of election spending reports**[60] – Depending on campaign finance requirements, the reports may reveal whether campaigns have used data acquisition services (such as data brokers and political advertising companies), had contracts with third parties for digital marketing and online advertising, thereby exposing the scale and nature of personal data utilization even when detailed targeting information remains opaque.
    - **Analysis of political ad libraries and transparency reports**[61] - This may help election observers track and understand the targeting criteria, intended and actual audiences, and parameters used to determine which voters received specific political messages, revealing the extent to which political parties or candidates utilized data-driven (micro) targeting and profiling of voters. It may also showcase paid promotion of various data collection tools.

60 See, for example, this case study by Tactical Tech: **Data and Democracy in the UK A report by Tactical Tech's Data and Politics Team**

61 See, for example, this case study by Tactical Tech: **The Transparency of Facebook Disclaimers in the 2022 Lebanon Elections**

- **EMBs** – Similarly to the one described above, this approach involves election observers systematically monitoring how EMBs collect, store, use, share, and protect voters' personal data throughout the electoral cycle. This may be done by attending EMB meetings, witnessing voter registration or voter identification procedures (during voting), reviewing data security measures and their implementation (such as cybersecurity training of election commissioners), monitoring interactions between EMBs and private vendors or contractors (for example, to assess the risk of unauthorized data sharing or inadequate oversight), and so on. When available, observers should also request access to election technology vendor documentation (see **NDI's Election Tech Toolkit** for more detail). Given the inherent opacity of many of these processes due to technologies used, direct observation methods come with important limitations described further in this chapter.
  - **Review of election technology vendor documentation** – Stronger transparency requirements exist with regards to procurement of election technology by the EMBs than those related to campaign technology. Observers may scrutinize available documentation to assess vendor access to data, details of its prospective and actual data processing activities, security safeguards, oversight mechanisms of the EMB, and so on. As with the adoption of any election technology, scrutiny should begin at the earliest possible stage – during procurement and before deployment – rather than waiting until the technology is already essential to the election process, to avoid dangerous dependencies and future difficulties in addressing problems.

- **Key informant interviews** – This method may help expand and inform findings of the direct observation method described above. For instance, interviews with campaign volunteers or lower-level EMBs could provide valuable insights into the actual practices of handling voter data that may remain otherwise "unobservable." Notably, interviewing the individuals who are as close as possible to the actual data collection and processing in the "field" could showcase how well the policies and directives of the national-level leadership are implemented down the line. Observers may also interview affected voters (data subjects).
  - **Expert interviews**[62] – Especially in cases when observers' have limited access to the election or campaign technology vendor documentation, interviews with industry experts may offer valuable insights into common methods, practices, and functionality of technologies available on the market.
  - **A hotline or another method for citizens to self-report incidents** – Granted that voters are sufficiently privacy-conscious or when privacy monitoring efforts are accompanied by a voter education effort, observers may consider establishing a self-reporting mechanism for voters to report potential personal data abuse.

- **Review of data protection policies**
  - **Election contestants** – This is a documentary analysis method that involves election observers systematically examining the written policies, procedures, and public commitments of political parties and candidates regarding their handling of voters' personal data. Observers may collect and analyze privacy policies, terms of service for campaign websites, apps and other instruments, and other publicly

62 See, for example, this case study by Tactical Tech: **Data-driven campaigning in the 2015 UK general election.**

available documentation to assess whether contestants have established clear policies governing data collection, processing, retention, security, and deletion. Notably, the absence of such information in the public domain is an important finding and would contradict most data protection regulations. In addition, pairing such analysis with direct observation of election contestants' actual practices could help observers identify important gaps between stated policies and their practical implementation.

- **EMBs** – This is a documentary analysis method that allows election observers to examine whether EMBs have established comprehensive data protection policies governing the collection, use, storage, and sharing of voter data. This may involve reviewing formal policies or holding meetings with EMB officials about their practices and challenges. The findings could be assessed for compliance with the local data protection regulations, specific guidance issued by the DPA for the EMBs, as well as against general data protection principles. Complimentarily to this method, observers may interview EMB officials on different levels about their data-centered practices or request information about complaints or investigations from relevant authorities.

- **Official requests for information** – This is a formal method frequently used by election observers in other contexts, it may be utilized to request information regarding data processing practices, compliance mechanisms, and oversight activities in elections from election management bodies, data protection authority, and other regulatory bodies. For example, observers may request data protection impact assessments, audit reports, vendor contracts, records of security incidents, enforcement actions, and complaint statistics to verify official claims. Understandably, the method's effectiveness depends on institutional transparency and legal frameworks governing information access. However, even when institutions refuse to provide information on the basis of absent or weak legal regulations – citizen observers should be allowed to access such information as trusted actors in the electoral process.

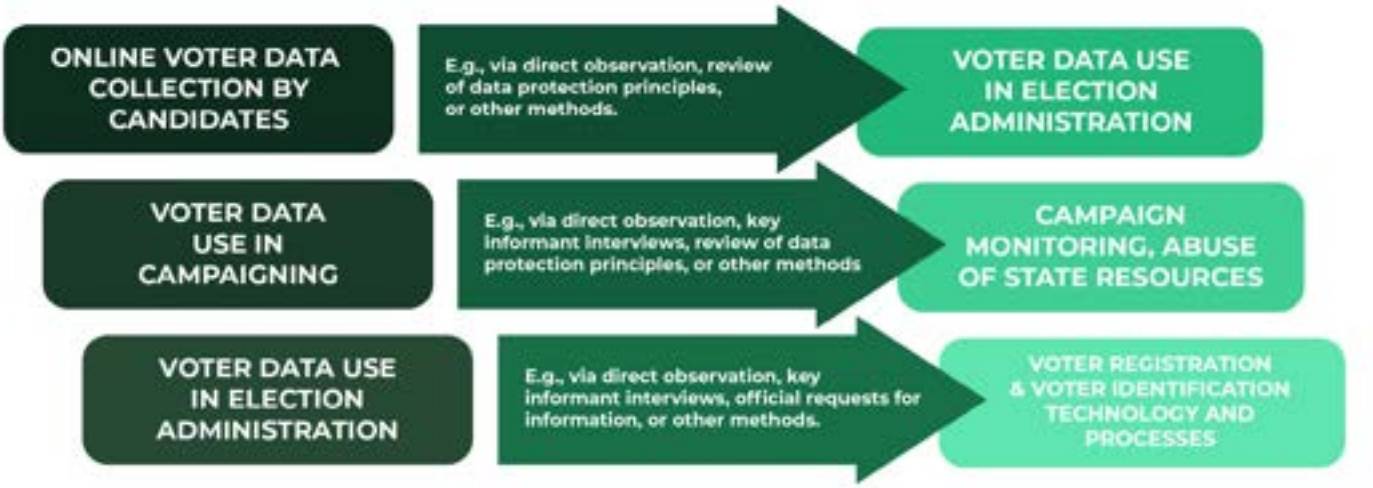
- **Assessments by the data protection authority (DPA)** – In complex or simply novel cases related to data protection issues, observers may seek an official opinion or assessment from the country's DPA, if one exists. This could help observers obtain authoritative interpretations of whether specific data handling practices by election contestants or EMBs comply with data protection law and identify potential violations that could undermine voter privacy and impact electoral integrity. However it's worth noting that in some contexts, DPAs are chronically under-resourced or politically captured. In cases where the DPA is weak or not perceived as independent, groups can also triangulate DPA assessments with academic consultations, and/or regional or international soft-law.

Standalone focus vs integration with existing observation methodology

As already mentioned, in some cases the use of personal data in elections may not warrant creating a standalone toolkit and deploying additional monitoring teams. Instead, observers may choose to integrate data protection considerations throughout their existing election observation elements and data collection mechanisms.

For instance, monitoring online data collection practices of election contestants may be integrated into social media monitoring or broader monitoring of election campaigning, including campaign finance and online political advertisements. Many organizations monitor

the abuse of state resources in the campaign, of which the use of personal data by state actors is notably relevant. In turn, monitoring personal data use in election administration can be integrated with broader monitoring of election technology, and so on.



Case Study: Personal Data Abuse in the 2022 Hungarian Elections

Human Rights Watch examined data-driven campaigning in Hungary's 2022 elections, which resulted in a fourth consecutive term for Fidesz and Prime Minister Viktor Orbán. The **report** documented how the Hungarian government repurposed personal data it had collected from citizens for administering public services including Covid-19 vaccine registration, tax benefit applications, and mandatory professional association memberships to spread Fidesz campaign messages. The research found that this misuse of state-collected data, combined with the capture of key institutions by the government, led to selective enforcement of laws that further benefited Fidesz, exacerbating an already uneven playing field and undermining citizens' right to privacy.

Observation Limitations

One-time, external, and superficial review of websites and other digital campaigning tools: Parties or candidates are unlikely to provide back-end access to their platforms and systems, while technology providers treat information about their products as proprietary, which leaves observers with only external access. Moreover, the functionality of a given website, app, or other digital tool may differ depending on user characteristics and means of accessing it (i.e., such as user device, browser, IP address, etc.). Furthermore, any assessment of a campaign website (or another online instrument, for that matter) represents a "snapshot" of its features at this particular moment in time, since technologies can get adjusted or updated at any point during a campaign. Therefore, when documenting findings, observers should carefully record the time of analysis and means of access. (Observers may also consider reviewing websites and other online technologies periodically throughout the election period).

No direct ("insider") access to information from campaign consultants or other industry representatives: Many of the practices and tools are treated as commercial trade secrets and remain opaque. Observers may be able to observe and document technology from a user

perspective but have little to no means to "reverse engineer" it. However, observers can (and should) highlight such limitations in their reporting and consider advocating against them with the use of international frameworks. [63]

Limited ability to assess security measures: Without backend access to technology, observers are only able to assess security controls and infrastructure of EMBs or election contestants through document review of vendor documentation, security protocols and audit reports, meetings with candidates and EMB officials, and examining whether independent security audits have been conducted or whether any security incidents have taken place. Observers should be extremely cautious of any external security assessment efforts, as in many places outside interference with online systems may be considered illegal, regardless of the intention behind it.

Inconsistent transparency requirements for technology platforms: Depending on the local legal and technological context, different social media and technology platforms may operate under varying rules and requirements, which creates inconsistencies in how voter data is protected or how transparency measures are implemented. This makes it difficult for observers to apply similar assessment criteria across different digital spaces.

Limited transparency requirements for election contestants: As discussed above, no specific guidance may exist regarding the use of voters' information by political actors altogether and/or they may be exempt from existing privacy laws. Other transparency obligations, such as existing campaign finance reporting requirements, may fail to adequately capture spending on data-centered campaigning practices or services. While a finding in itself, in these contexts observers are otherwise constrained in their ability to monitor the use of voters' personal data by election contestants.

Limited or no access to technology vendor documentation: As election technology is commonly considered proprietary, full vendor documentation may not be made publicly available even during a procurement process by an EMB. As discussed above, even more opacity exists around the tools offered by data brokers and political consulting firms.

RESOURCE CONSIDERATIONS AND TECHNICAL EXPERTISE

Monitoring the use of personal data in elections requires some specialized expertise, making careful resource planning essential when developing observation methodologies. Some of these skills organizations may already have in-house or could easily acquire, and these needs should not deter observation. Organizations must assess their available technical, legal, and analytical capacities and determine whether to build in-house expertise, partner with specialized organizations, or engage external consultants to effectively examine data protection practices in electoral processes. The following areas of expertise are particularly important for a successful data protection monitoring effort:

- **Legal expertise in data protection and electoral law** – Observers will need to have someone on their team with a deep understanding of applicable data protection

63 "Private companies providing such election technology should waive commercial confidentiality and make their technologies fully auditable to enable wide understanding of the functions and capabilities of the system," par. 4.7.13., page 14, **Guidelines on the protection of individuals with regard to the processing of personal data for the purposes of voter registration and authentication**, Council of Europe.

(such as national privacy laws or applicable regional frameworks like GDPR) and other relevant regulations (for example, personal data disclosure or protection requirements in the election law, freedom of information, cybersecurity, or online media legislation) and how they could impact the use of personal data in elections.

- **Understanding of technologies used in election administration** – To analyze the use of personal data in election administration, observers may need someone who can analyze procurement documents, vendor contracts, or technical specifications related to the technology utilized by EMBs. This may include having a tech practitioner/coder on the team, a data scientist, or someone with an understanding of technology that uses biometrics.
- **Understanding of data-centered campaigning methods and tools** – Observing data protection in election campaigning calls for a degree of familiarity with modern campaign tools including social media advertising platforms, CRM systems, mobile campaign apps, (micro)targeting techniques, etc.. However, observers may also utilize expert interviews or engage technologists to gain deeper insights or analyze particular tools.
- **Data analysis, OSINT, digital security, and other specialized expertise** – Depending on selected monitoring methods, observers may require a mix of other skills, ranging from data analytics, to OSINT investigation methods, to the understanding of digital security principles and their implementation.
- **Staffing and financial resources** – Most data collection and analysis of digital data collection and processing practices can be done centrally with a team of a relatively small group of monitors. The size of the team depends on the scope and the methods of the effort. Organizations should also consider how their monitoring activities intersect with other observation areas. For example, some organizations task their long term observers with conducting key informant interviews. The monitoring team would need to be well-trained with some specialized detection skills, and budgeted for throughout the duration of the monitoring project. When integrated with other observation areas, budgeting for the data protection monitoring within the overall election observation budget allows costs to be shared, for example, when it comes to administrative costs, project management costs, etc. Observers should also consider other financial resources required for such monitoring effort, including the costs of subscribing to various tools.
- **Timing of the monitoring effort** – Although the actual duration of monitoring data protection in elections may vary depending on the context, most of it is likely to fall within the long-term observation period. Notably, observing data protection in elections is most insightful and impactful when it involves real-time monitoring of ongoing campaigns and election administration processes.
- **Piloting new methodologies** – As with any update to a monitoring effort or introduction of new elements, election observers may plan for a "pilot" phase first, ideally during a non-critical electoral period, which will allow monitors to test data collection and analysis tools and methods, and refine methodologies as necessary before more earnest observation begins.

LEGAL, ETHICAL, SECURITY AND OTHER CONSIDERATIONS

Technology and security: Although there is an abundance of publicly available scanning tools for identifying security vulnerabilities on websites or other platforms – observers should be extremely cautious of external security assessment efforts, as outside interference with online systems may be illegal, regardless of the intention behind it. The definition of what constitutes an illegal interference may vary depending on local regulations, particularities of utilized tools, and technologies analyzed. Publicly disclosing sensitive findings of security assessments may also lead to various repercussions.

Working with sensitive findings / sensitive data: If any security vulnerabilities or incidents come to light, publicly disclosing those (i.e., in an election monitoring report) may bring further harm to voters (data subjects) or expose data processors to further attacks, as well as sometimes lead to legal repercussions. In such cases, observers may consider sharing sensitive findings directly with monitored entities or otherwise narrowing the circle of recipients. In such cases, findings may be paired with tailored recommendations, implementation of which can also be the subject of analysis.

Similarly, observers may come across or be called to investigate allegedly illicitly obtained or leaked datasets containing information about voters. They should come up with a protocol for handling such cases that may include documenting the steps of an investigation and limiting internal access to this data.

In any case, when publicising their findings, observers should take care not to inadvertently reveal personal data of voters or other observation subjects.

Implications for own data protection practices: Monitoring data protection in elections may prompt internal review of data handling within election observation organizations or coalitions. Observers should remember that publicising findings of monitoring may also prompt public scrutiny of these matters related to the observers themselves.

UNDERSTANDING AND COMMUNICATING FINDINGS

With such novel topics as data protection, observation findings publicised without a clear strategy may be poorly understood by the public, stakeholders, and journalists, taken out of context or sensationalized by the media. Therefore, it is critical that observers take some time to think through how they would assess and communicate what they found to the public. Here are a few recommendations to consider:

Clear communication despite complexity:

- First, observers should think carefully about what they actually found and what their findings “mean” for election integrity. When unsure about how to assess prospective impact on the electoral process, ground the analysis in the electoral integrity standards. For example:
    - Voter disenfranchisement through inaccurate voter lists or profiling

- Uneven playing field for political contestants
- Voter manipulation through opaque (micro)targeting
- Discriminatory exclusion based on profiling characteristics
- Violations of voter privacy and political opinion[64] confidentiality through profiling, including via data inference

- Any communication of findings should be done in plain and accessible language, alongside explaining specific concepts used, such as data brokers, voter profiling, (micro)targeting, and so on.
- Clearly describing observation methodology and the key principles followed should be part of the communication strategy and materials.
- If any findings are too sensitive to share with the broader public – i.e., those concerning data security – observers should think about who should be provided full information and what sensitive detail should be removed before publication (see the section on Legal, ethical, security, and other considerations above for more detail).

Multi-stakeholder communication: related to the above, observers may want to think about communicating findings beyond just the public and traditional electoral stakeholders. For example:

- **Data Protection Authority:** Share complaints and systemic findings about personal data misuse
- **Election Management Bodies:** Communicate election-process related concerns, such as voter list management, vendor oversight, or procurement transparency
- **Political parties and candidates:** Alert them to violations of data protection principles in their campaigns
- **Technology vendors:** Notify companies providing electoral technologies (biometric systems, results transmission systems, voter databases) about security vulnerabilities or data protection gaps.

Notably, different stakeholders might require different communication styles due to their different levels of familiarity with the topic.

Aligning communications strategy and schedule with methodology: The monitoring methodology should drive observers' communications schedule. For instance, if the methodology includes monitoring voter registration systems, procurement processes, or campaign data practices, plan to release findings after completing each phase of data collection and analysis.

64 Under modern data protection laws, personal data revealing political opinions is a special category of data, the processing of which is subject to strict safeguards. Generally, processing of such sensitive data is prohibited unless the affected data subject provides explicit, specific, fully-informed and freely given consent to such processing. (See **the CoE Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns**, par. 4.2.)

Communicating sensitive findings: As discussed in the section on legal, ethical, and security considerations, observers may consider sharing sensitive findings directly with monitored entities or otherwise narrowing the circle of recipients instead of including this information into regular public statements or reports. Observers should also take care not inadvertently reveal personal data of voters or other observation subjects when publicizing findings.

CHAPTER 6: MAKING AN IMPACT WITH DATA PROTECTION MONITORING

Stakeholders look to election observers to provide recommendations to address any shortcomings they identify in the process. The recommendations can serve as the basis of reform initiatives, and ongoing benchmarks for future elections. Observers should be prepared to offer recommendations as part of their data protection monitoring, which may be regulatory, behavioral, or otherwise. Like all recommendations, these should be specific and actionable which may take some understanding of the broader policy framework around data protection and privacy. In addition, recommendations often require broader advocacy efforts to truly take root with relevant stakeholders.

Additionally, as with any new and complex areas of elections, observers should keep several considerations in mind when formulating recommendations.

CONSIDERATIONS WHEN FORMING RECOMMENDATIONS

- **Rapidly evolving campaign technologies and data practices:** The rapid advancement of campaign technologies has outpaced regulatory frameworks in many jurisdictions, meaning that existing legal frameworks often **fall short either in substance or enforcement**. This also makes formulating recommendations difficult as they can become outdated very quickly. While recommendations should be specific, they should also be written with longevity in mind, which may mean grounding recommendations in principles and avoiding being overly prescriptive.

- **Different (conflicting) frameworks and oversight bodies:** Examining data protection in elections necessarily expands the legal framework that observers will need to analyze and consider. There are numerous pieces of legislation that could apply to data privacy in elections – for instance, data protection laws, political party laws, electoral laws, and possibly other cybersecurity legislation, and these may not always align which can lead to inconsistent or confusing application. In addition, in many jurisdictions, no specific guidance exists regarding the use of voters' information by political actors, and/or the latter are exempt from existing privacy laws.[65] Gaps and different legal constituencies can present challenges with enforcement and to crafting recommendations that recognize the complexity of the framework. However, this should not preclude observers from recommending appropriate data protection mechanisms to public bodies and political actors. Such as conducting a Data Protection Impact Assessment (DPIA)[66], especially when undergoing digitalization or adopting new election technologies or appointing an internal Data Protection Officer (DPO).

- **Diverse regulatory contexts globally:** Data privacy regulations vary drastically from country-to-country, making presenting comparative information or promoting unfamiliar concepts and protocols difficult. Additionally, some jurisdictions may still not have any personal data protection regulations.

65 **Technology, Data, and Elections: A Checklist on the Electoral Cycle**, Privacy International.
66 For example, see the guidance from the **UK Information Commissioner's Office** and the **European Data Protection Supervisor**.

- **Avoiding misinterpretations that could diminish transparency:** Observers should take extra care to ensure that data protection recommendations are conceptualized and drafted in a way that they cannot be misconstrued to obstruct observation of electoral processes, which would ultimately undermine transparency and/or accountability.
- **Platform-specific regulation inconsistencies:** Different social media and technology platforms operate under varying rules and requirements, creating inconsistencies in how voter data is protected or how transparency measures are implemented across different digital spaces. In addition, platforms are often quiet when they change or update their data protection protocols, or it's buried in a long, legalese user agreement, which may make it harder to accurately target these platforms with recommendations.
- **Disconnect between legislative intent and actual campaign practices:** There is also a disconnect between legislative intent and actual campaign practices, as election contestants find creative ways or "loopholes" to circumvent the spirit of data protection laws while technically remaining within their bounds.

Challenges to enforcement: Even where comprehensive regulations do exist, enforcement often proves challenging due to the speed and complexity of digital campaign operations, the cross-border nature of many data processing activities, and the difficulty of detecting violations in real-time. This creates a situation where even well-intentioned privacy protections may fail to achieve their intended effects, leaving voters' data vulnerable to misuse despite the existence of formal safeguards.

POLICY AND ADVOCACY

Election observers can use data protection principles and data subject rights as both **an evaluative framework** and **an advocacy tool** to assess whether electoral processes adequately protect citizen privacy and uphold democratic election principles.

When engaging in post-election advocacy and reform efforts, observers need to consider the following aspects.

Voter awareness raising: While electoral integrity principles are universal, data protection issues and discourse around them are somewhat cultural - i.e., in some societies people are more attuned to those rights than others. Especially in societies where awareness is low or privacy has not culturally been a big concern, observers may want to dedicate more efforts to public awareness raising about the importance of personal data protection in elections and otherwise.

As mentioned above, citizen observers are uniquely positioned to bridge the critical knowledge gap between the public, government officials, and electoral actors regarding how personal voter data is collected, processed, and deployed throughout the electoral cycle. This awareness-raising role is essential because most voters have limited understanding of how their information might be combined, processed, or shared once collected, or how data-driven targeting and profiling techniques are used to influence their political opinions and behavior.

The need to distill a complex issue: However, to be successful in both public awareness raising and advocacy, observers will have to translate complex technical issues into accessible information, helping stakeholders understand the implications of data practices for electoral integrity. This presents both a challenge and an opportunity for election observers. While the technical aspects of data collection, processing, and targeting can be difficult to explain, privacy concerns often have strong bipartisan resonance that transcends political divides, which makes data protection an effective entry point for advocacy.

Building a partnership with the data protection authority: Where available, observers can strategically engage the DPA at multiple stages of the observation and advocacy process. For instance:

- During the monitoring, the DPA can help observers understand complex regulatory frameworks and identify potential violations as well as share information about complaints related to electoral data use;
- Ahead of presenting the findings, the DPA can validate technical assessments and legal interpretations, as well as help formulate recommendations, while engagement during presentation of the findings could add regulatory credibility to observer findings;
- During further advocacy efforts, the DPA can help translate observer recommendations into enforceable standards, issue special guidelines on personal data use for candidates and campaigns, and provide ongoing guidance and support for public education initiatives.

Building partnerships with other interested groups: Effective advocacy for election integrity through data protection requires coalition building with diverse stakeholders. Among them, observers may consider:

- **Civic Tech Organizations** – can provide technical expertise on data systems, algorithms, and digital platforms, help develop monitoring tools and methodologies for tracking data use, offer insights into emerging technologies and their implications for elections, or help prescribe standards for promoting privacy-by-design approaches;
- **Human Rights Organizations** – can help frame privacy issues within broader human rights frameworks and commitments, especially with regards to collection and processing of data of vulnerable groups;
- **Consumer Protection Organizations** – can bring experience in data governance and individual rights enforcement, as well as help observers understand commercial data broker practices and targeting techniques from a variety of perspectives (i.e., form a viewpoint of child and adolescent online health and safety). These organizations can also assist with tracing connections between consumer data collection and political profiling;
- **Advocacy and civil liberties organizations, tech researchers, and academia** – can bring specialized expertise in data protection laws, privacy rights, and surveillance practices, can conduct independent research, investigation, and policy analysis on data processing activities, or provide educational resources and awareness-raising on privacy rights and data exploitation. They can also engage in strategic litigation to challenge violations and establish legal precedents for data protections.

CHAPTER 7: LOOKING FORWARD

EMERGENT ISSUES IN DATA PROTECTION AND ELECTION OBSERVATION

This guide has covered several challenges that data protection poses to electoral integrity, and ways observers can help build transparency and accountability around the use of personal data in elections. Observers will need to be prepared to continuously reexamine the data protection context of their elections as technologies and their uses evolve, as well as in response to changing commercial practices, policy developments, and regulatory frameworks. This also involves being forward-thinking and anticipating innovations, while considering how broader technological trends may impact elections. This may include:

Data privacy and AI: The companies developing Large Language Models (LLMs) are the same tech giants that already operate under a business model based on collecting, analyzing, and selling people's data (so-called '**surveillance capitalism**'). LLM development fundamentally relies on analyzing large amounts of data, often derived from indiscriminately scraping terabytes of online content from news sites, blogs, social media and anywhere they can reach, often without proper rights to use it. For example, Google admits to training AI models on YouTube content, while Meta integrates AI into services using billions of images and videos from Instagram and Facebook to train its models. Companies are generally secretive about training data sources, quietly changing privacy policies to expand what data can be used for AI training. Many people producing content online don't know about or have not agreed to it being used for LLM training - including older content (2022 and earlier) which has already been scraped and captured prior to any new disclosure interventions. The challenge is balancing the demand for data to train powerful LLMs with indiscriminate mass scraping of personal information that may infringe on privacy rights. In addition, most very large online platforms behind LLMs lack local representation and fall outside the national jurisdiction of a country. This poses practical obstacles for oversight and enforcement. For more information about monitoring the use of generative AI in elections, see NDI's accompanying guide "**Synthetic Voices, Real Voters: A Guide to Monitoring Generative AI in Elections for Nonpartisan Citizen Observers**."

Exponential growth of data available for political campaigning: As data-centric technologies continue to proliferate, **the sheer volume of data collected about users is bound to continue to grow exponentially**. For example, it is conceivable that the data collected about the users of smart home systems, wearables, connected vehicles, and Internet of Things (IoT) devices would also be utilized for election campaigning. The challenge lies in the fact that many of these devices live in private spaces and collect highly intimate data, while voters may have limited awareness of how this information could be accessed or used for political purposes. Election observers will need to develop methodologies to assess whether campaigns are accessing IoT data sources and evaluate the transparency and consent mechanisms around such practices.

Foreign malign election interference and data protection: As discussed above, increased adoption of digital voter registers and other data-centric technology drives corresponding security risks of data breaches, leaks, and hacks by malign actors. This is evidenced by a growing number of cases when hackers successfully infiltrated state and local election databases,

manipulated voter records, or stole them to target voters with false narratives or intimidation campaigns. For example, in 2021, Chinese state-backed hackers **compromised the UK Electoral Commission's systems**, accessing the personal information of approximately 40 million UK voters. In 2021, the US **charged two Iranian hackers** for attempting to compromise voter registration and information websites and engaging in voter intimidation campaigns during the 2020 election. It is likely that such cases will only increase, while the millions of records that have already illegally ended up in foreign hands would be used for manipulating elections in the future. Hence, election observers, civil society organizations, and other actors working to counter foreign interference will have to increasingly prioritize monitoring data protection practices, including cybersecurity, as essential components of electoral integrity.

It is also worth noting that despite ongoing innovation of technology, observers should not lose focus on data-centric practices that use non-digital tools, such as paper-based records. In their assessments and recommendations, observers should also keep in mind that not every issue needs a "technology" solution and that some recommendations may as well consider moving away from or not adopting the latest technological tools, especially if their use may jeopardise citizens' privacy or other voters' rights.

Consideration for Data Protection within an Election Observation Organization

As citizen election observation organizations engage in monitoring data protection in electoral processes, they must recognize that this work carries important implications for their own operations. Observers who publicly evaluate the data handling practices of election management bodies, political parties, and other electoral actors should anticipate that their own data protection standards and practices will come under similar scrutiny from governments, political actors, and the public.

This heightened attention creates both a responsibility and an opportunity: observation organizations must ensure their internal data practices meet or exceed the standards they advocate for others, including how they handle data of their own observers and staff. At minimum, election observers should implement the same data protection principles, security measures, and transparency practices they use to assess other electoral stakeholders – anything less risks undermining their credibility and potentially exposing citizen election observation organizations to the very data protection violations they seek to prevent.

Citizen election observers should view this as an opportunity to strengthen their institutional capacity, build trust with stakeholders, and model best practices in an increasingly data-driven electoral environment. Most importantly, observers may simply want to ensure they treat people's personal data fairly, with respect, and in accordance with legal requirements.


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


Sida