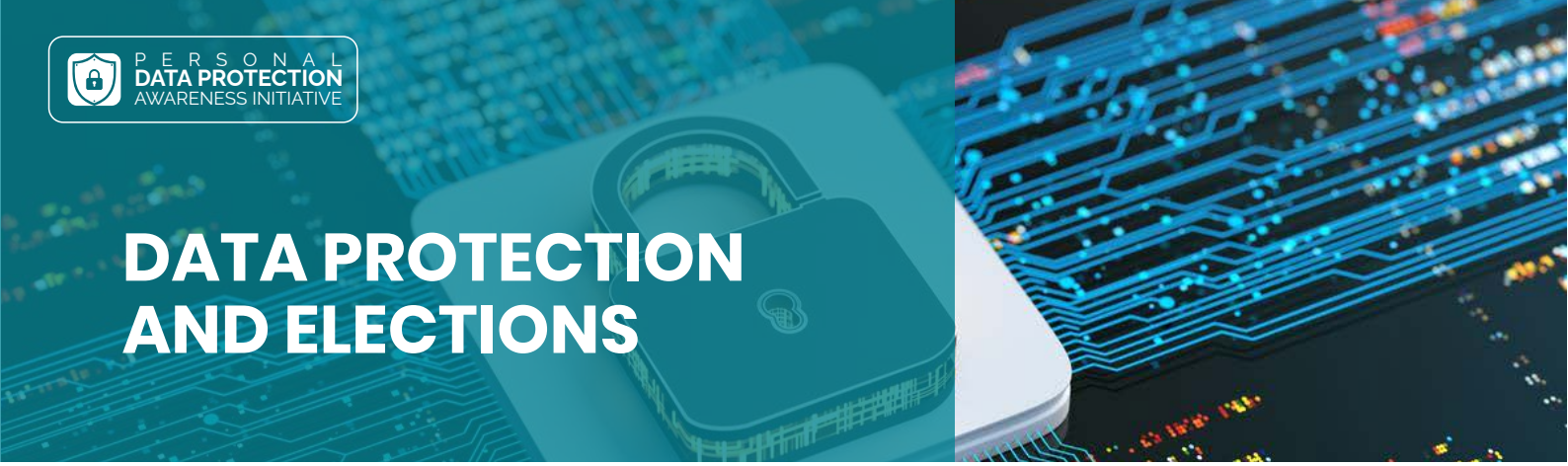
PERSONAL DATA PROTECTION AWARENESS INITIATIVE



DATA PROTECTION AND ELECTIONS

Introduction

During the season of any nation's general elections, different groups, such as electoral bodies, political parties, election monitors or observers, etc., have to deal with a lot of personal information about the electorate. Since we are in an era where many day-to-day activities have gone digital, democratic engagement has been increasingly mediated by digital technology. Hence, the effects of unlawful personal data processing during elections have become far-reaching. So, it is very important that data protection rules are followed when handling personal information. This piece will focus briefly on the activities of electoral bodies and political parties.

The Electoral Body

Nigeria is now in the month of its general elections. But before this election, the body in charge of elections, the Independent National Electoral Commission (INEC), had been doing things like registering people who were eligible to vote and making PVCs. From the point of view of data protection, the Commission can only process personal data if it has a legal bases to do so. For instance, it can handle personal information if doing so is in the public interest. According to the NDPR, art. 2.2(e), and the GDPR, art. 6, "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." For this basis to work, the public interest must be rooted in a national law that meets an objective or public interest and is proportionate and legal for the goal that is being pursued.

Even though INEC's activities fit within this legal basis, it must also follow the principles of data processing. These are the principles of lawfulness, transparency, fairness, purpose limitation, data minimization, accuracy, storage limitation, security, and accountability. Keeping these principles in mind, a couple of issues are pertinent.

INEC is currently processing both personal and special types of data, such as biometrics. But we don't know what security measures have been put in place to protect people's sensitive data. We are also not aware if the Commission conducted a data protection impact assessment exercise to determine the level of risk their processing will occasion and proffer ways to mitigate it. Does INEC use third-party service providers for both voter registration and the actual voting? Most likely, yes. What are the data protection practices of these companies? Are their digital tools embedding privacy by design? The Commission's official website doesn't have a privacy notice, and the App's privacy notice doesn't say what lawful bases they process data on, what rights data subjects have, or how they can use those rights or make a complaint. These are the issues.

Political Campaigns

In the GDPR, which is some sort of global standard, Recital 56 elaborates on processing personal data for election purposes, particularly the processing of personal data on people's political opinions by parties. It says that "*where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.*"

Political parties now have apps to maximise support, disseminate information to supporters, etc., which is not a bad thing as effective political communication through political campaigning is central to democratic forms of government. Voters need to know about the candidates and political parties, as well as what their plans and policies are for the future. With the help of digital advancement, political aspirants can connect with voters and get them to vote more effectively, as they have better information about voters' beliefs, preferences, and dispositions.

However, trust and confidence in the integrity of elections can be undermined by hidden practices that permit the manipulation of data on the electorate for the delivery of such focused messages. Most countries' elections are becoming more "data-driven," so it's very important that all groups involved in the election process handle personal information about voters in line with well-known data protection principles. Questions on data protection are now at the center of discussions about the strength and stability of democratic institutions and the rights to free elections that are written into human rights instruments.

Challenges of Using Digital Technology for Election Related Activities

Cyber-attacks are more likely to occur during elections in which digital technology is used throughout the campaign and election process. The most important effect of this digitalization is that measures to protect against cyberattacks need to be thought about for the whole election campaign and process, from setting up the electoral registry to e-voting, from the voter and supporter databases managed by political parties to the data collected and used by social media platforms, data brokers, and the ad tech industry. This raises the question: What safety measures have INEC and political parties put in place to protect sensitive personal information about people?

Conclusion

While we hope that, before the next election in 2027, the regulator, the Nigerian Data Protection Bureau (NDPB), will issue guidance to electoral officers, political parties, and other election actors on data processing during periods of election, it is important that all actors within the election process comply with data protection principles. Data subjects also need to be more data protection conscious, particularly with their PVC. For example, they should not share an unredacted copy of their PVC on social media.

PERSONAL
DATA PROTECTION
AWARENESS INITIATIVE