

What does the protection of personal information act, 2013 mean for south African elections?

1 May 2019 5 min read

by Ahmore Burger-Smidt, Head of Data Privacy Practice and Mahlogonolo Motimele, Candidate Attorney

A CLOSER LOOK AT THE VOTERS ROLL

POPIA applies to the processing of information, by automated and non-automated means, by persons domiciled in the Republic or persons using processing means in the Republic^[1], this includes political parties. The planning, implementation and management of elections involves the processing of voters' personal information, and thus POPIA is automatically invoked.

Data subjects receive not only calls and SMS messages, but at times emails from various political organisations. The question then becomes, where did the political party get one's personal information? Who gave the party permission to use a person's personal information? When was consent received as envisaged by POPIA? More importantly, why is it that political organisations wish to know how and whether we wish to exercise the right to vote at all?

At the heart of the debate is the fact that the voters' roll is a public document in South Africa that can be accessed by any political affiliation and any person at the mere payment of a fee.^[2] Furthermore, it is available at the Electoral Commission's head office for inspection during office hours.

The voters roll contains important and private information such as a person's name and surname, identity number, cell phone number, address, date of birth, as well as the voting district in which a person will cast their vote. The very inclusion of one's identity number provides details of one's date of birth, gender, age as well as whether a person is a South African citizen or a permanent resident. Also, one might very well object to one's mobile number being available at the offices of the Electoral Commission.

The information in the voters' roll most definitely raises various questions when considering the right to privacy and POPIA in general.

In addition to the voters' roll, individuals willing disclose and share personal information on a daily basis on public platforms and social media and do not question the impact of disclosing personal information on their daily lives.

The use of voter's personal information by political parties to campaign is not a concept that is unique to South Africa. For instance, the Information Commissioner's Office in the UK ("ICO") published a report in 2018 regarding the progress in an investigation regarding data brokers, i.e. businesses that collect personal information and then on-sell it, in political campaigns. Also, in the UK, it was discovered that political parties use online platforms such as Facebook and Google for their political campaigns and do so by using personal information to target a particular audience. The ICO is in the process of developing codes of practice for political parties and has developed a guideline for political parties, which was published on 11 July 2018.^[3]

The South Africa information regulator, Advocate Pansy Tlakula, at the International Conference of Information Commissioners 2019 conference, reiterated the need for developing a guideline in respect of access to information and the protection of personal data in the election process. The issue of personal data and how it is used in the election process truly is a burning issue.

Political parties around the world rely to a certain extent, on data and personal data. They rely on data, voters' data, to facilitate and inform their decision-making. Amongst others voters data is used to make decisions as to which campaign messages to focus on or how to target supporters, undecided voters, and non-supporters.

While data driven political campaigns are not in any way or manner new, the extent and granularity of data available and the potential power to sway voters through that data is.

From a POPIA perspective, the use of personal data when it comes to political campaigning is highly privacy invasive and indeed raises important data security questions. Furthermore, the use of personal data could very well undermine faith in the democratic process.

There is a complex corporate ecosystem behind targeted political advertising. This isn't just Facebook, but also data analytics companies that should stand up and be part of this important conversation. Data analytics firms are employed by political parties contesting elections to inform the campaign direction of the party. What drives this process is not always clear to a voter.

What is, however, clear is that there are companies whose business model it is to analyse and in some instances exploit the data people share in the public domain in such a way that intimate personal details about a person's beliefs, habits, and behaviour can be better understood and used for the purpose of allowing political parties to target these individuals with political messages.

Access to personal information and the use thereof should be top of mind to every single voter, not only in South Africa, but all over the world.

POPIA in South Africa will have an impact on how political parties' access, process and use voters' information going forward. Therefore, at minimum, political parties should educate themselves and their members about what is required from them in terms of the soon to be in force data protection laws. The protection of personal data should be at the center of their functions and activities and their actions must show that not only is your vote important to them, but they recognise the sensitivity and value of the population's information and respect your privacy.

[1] Protection of Personal Information Act, 2013, Section 3 (1) (a) and (b).

[2] Electoral Act 73 of 1998, Section 16.

[3] "Information Commissioner's Office, Democracy Disrupted? Personal Information and Political Influence", 11 July 2018 accessed at the ICO website.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)