



---

## 2021 YEAR END UPDATE

Christmas is around the corner and 2021 unlike its predecessor has been nothing short of eventful. New legislation like The Protection of Personal Information Act ("**POPIA**") came into effect fully on the 1st of July which saw companies scrambling to ensure that they were compliant. Despite the regulation of data by the POPI Act, South Africa still experienced a record number of cyber breaches throughout the year with breaches such as the ransomware attack at a debt recovery services firm called Debt-IN Consultants which is used by most local banks or the most notable breach by Credit Bureau Experian which exposed personal information of as many as 24 million South Africans and 793 749 business entities to a suspected fraudster. The Department of Justice ("**DOJ**") also experienced a data breach on the 6<sup>th</sup> of September 2021. This breach affected the Information Regulator ("**IR**") which relies on the DOJ's IT systems for its own operations making its website unavailable for three days, and the e-mail system also went offline. This is proof that no organisation is safe from cyber-attacks. Due to increased digitalisation companies are encouraged to take all the precautionary measures to ensure that their systems are protected from cyber-attackers. Despite the official commencement of the Act and the host of data-breaches experienced in 2021 we have not seen any penalties or arrests being made by the Information Regulator for non-compliance with the Act.

On the 1<sup>st</sup> of December 2021 we saw certain sections of the Cyber Crimes Act of 2020 ("**CCA**") coming into effect. The CCA aims to:

- create offences which have a bearing on cybercrime;
- criminalise the disclosure of data messages which are harmful and to provide for interim protection orders;
- deal with jurisdictional issues in respect of cybercrimes;
- regulate the powers to investigate cybercrimes; and
- impose obligations to report cybercrimes.

To name a few things.


The CCA creates 20 new offences such as hacking, ransomware, and malicious communications. It also creates penalties such as a fine (not specified) or imprisonment for a period of one to fifteen years. The CCA above POPIA creates greater obligations for companies and they need to educate themselves on the new regulations in order to ensure compliance.

In 2021 the Financial Sector Conduct Authority ("**FSCA**") conducted a lot more audits. We also saw a lot more communication from the FSCA than in 2020 with Requests to Provide Information from the FSCA and Directives to Provide Information for the Financial Intelligence Centre ("**FIC**"). As the regulatory requirements increase, companies are urged to ensure that their houses are in order as they will face more scrutiny from regulators such as the FSCA and the Information Regulator in the coming year.

*Remember when disaster strikes, the time to prepare has passed.*

*Steven Cyros*

**Lethubuhle Ncube**

 +27 (0) 63 912 6612

 [lethubuhle@corporatecounsel.co.za](mailto:lethubuhle@corporatecounsel.co.za)

 <http://www.corporatecounsel.co.za/>

