WERKSMANS
ATTORNEYS

EMPLOYMENT

Powers of the Information Regulator and how the Department of Justice could have avoided a R5 million fine

2 August 2023 *4 min read*

There has been great anxiety amongst organisations since the Protection of Personal Information Act 4 of 2013 (**POPIA**) came into effect two years ago. Many feared there would be immediate significant fines by the Information Regulator (**Regulator**) for non compliance with POPIA. However, that was not the case which caused the great anxiety to turn into quiet doubt about the Regulator's powers and appetite for enforcement, until recently.

The Regulator is empowered by POPIA to monitor and enforce compliance by public and private bodies. Where there is non compliance with POPIA the Regulator may issue an infringement notice specifying an administrative fine payable by the offending party. This begs the question of how organisations find themselves facing a fine by the Regulator. Further, it begs the question of what more can the Regulator impose on organisations facing enforcement.

In a recent article we discussed how the Regulator had just fined the Department of Justice and Constitutional Development (**DoJ**) R5 million for not having appropriate security measures to protect the personal information it holds. What is interesting is that after investigating the DoJ and finding that it had failed to comply with POPIA, the Regulator issued an enforcement notice. An enforcement notice empowers the Regulator to compel non compliant organisations to take specific remedial steps to rectify their non compliance. This can be viewed as a statutory olive branch. However, on the other side of the olive branch is a thorny end which the Regulator turns to once an organisation, through inaction by its employees, fails to comply with an enforcement notice. This is what happened in the DoJ's case and that is what led to the fine.

In issuing the infringement notice the Regulator not only fined the DoJ but also went further to not just recommend, but in fact require the DoJ to institute disciplinary action against employees who failed to renew the antivirus software and other security software. The DoJ will have to ensure that any such action is compliant with the requirements of South African labour law and its own internal codes and policies, but it would not be surprising if a number of employees, from any specific staff member tasked with ensuring security software is up to date and lawfully licensed, to any manager ultimately responsible for the DoJ's IT environment, could face serious disciplinary allegations of gross negligence or other failure to provide sufficient oversight. Given the materiality of the possible fine, and the risks of consequential damages, such disciplinary action could even extend to dismissal.

The risk to employees does not end with disciplinary action. The Regulator clearly stated in its media release relating to the DoJ fine that failure to abide by an enforcement notice may also result in liability upon conviction to a fine or to imprisonment of the **responsible officials**. This is in line with section 103 read with section 107 of POPIA. In particular, these provisions provide that any person convicted of an offence, such as failing to comply with enforcement and information notices, is liable to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment. As such, it is important for employees to note that the buck does not stop with the organisation when it comes to compliance with POPIA. It can be passed back to them meaning that they may be held personally responsible for POPIA offences which can result in dire consequences. Therefore, it is not only important for organisations to have a reasonable privacy framework in place but also to train their employees on data protection (and for employees to behave accordingly).

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Bradley Workman-Davies

Director

View Profile