Enforcement Notice issued to Dis-Chem due to contravention of PoPIA

On 31 August 2023, the Information Regulator (Regulator) issued an Enforcement Notice to the Dis-Chem Pharmacies Ltd (Dis-Chem) following the finding of the contravention of various sections of the Protection of Personal Information Act (PoPIA).

Photo by Pixabay via www.pexels.com

Around April and May 2022 Dis-Chem's third-party service provider, Grapevine, suffered a brute force attack by an unauthorised party. A brute force attack is aimed at cracking a password by continuously trying different combinations until the right character combination is found. On 1 May 2022 Dis-Chem became aware of the security compromise, or data breach, through SMSs sent to some of its employees, and on 5 May 2022, Dis-Chem then notified the Regulator in writing of this security compromise.

Approximately 3.6 million data subjects' records were accessed from Dis-Chem's e-Statement Service database which was managed by Grapevine. The affected records in this database were limited to names and surnames, e-mail addresses, and cellphone numbers of the data subjects (the individuals to whom the personal information relates).

The Regulator then conducted an own initiative assessment into the security compromise following Dis-Chem's failure to notify data subjects as required by section 22 of PoPIA. Following the assessment, the Regulator determined that Dis-Chem had interfered with the protection of personal information of the data subjects, and thus breached the conditions for the lawful processing of personal information.

The Regulator's assessment found that Dis-Chem failed to:

- identify the risk of using weak passwords and prevent the usage of such passwords.
- put in place adequate measures to monitor and detect unlawful access to their environment.
- enter into an operator agreement with Grapevine and ensure that Grapevine has adequate security measures in place to secure personal information in its possession. Furthermore, the agreement would have outlined processes of reporting to Dis-Chem in the event of a security compromise.

Accordingly, the Enforcement Notice issued by the Regulator orders Dis-Chem to, among others:

- conduct a Personal Information Impact Assessment to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information as required by Regulation 4(1)(b) of PoPIA.
- implement an adequate Incident Response Plan. implement the Payment Card Industry Data Security Standards (PCIDSS) by maintaining a vulnerability management programme, implement strong access control measures and maintain an Information Security Policy.
- ensure that it concludes written contracts with all operators who process personal information on its behalf, and that such contracts compel the operator(s) to establish and maintain same or better security measures referred to in section 19 of PoPIA.
- develop, implement, monitor, and maintain a compliance framework, in terms of Regulation 4(1)(a) of PoPIA which clearly makes provision for the reporting obligations of Dis-Chem and all its operators in terms of section 22 of PoPIA.

Dis-Chem must provide a report to the Regulator on the implementation of the actions ordered in the Enforcement Notice within thirty-one (31) days of the issuing and receipt. Should Dis-Chem fail to abide by the Enforcement Notice within the stipulated timeframe, it will be guilty of an offence, on which the Regulator may impose an administrative fine of an amount not exceeding R10 million or be liable upon conviction to imprisonment or both.