FORM 15

ENFORCEMENT NOTICE IN TERMS OF SECTION 95 OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 12(2)(c)]

Reference number: SC 30/2022

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject/complainant/aggrieved party:	The Information Regulator (South Africa) Own initiative assessment in terms of section 89(1) of the Protection of Personal Information Act 4 of 2013 (POPIA)
Unique Identifier/ Identity Number	N/A
Residential, postal or business address:	JD House
	27 Stiemens Street
	Braamfontein
	2001
Contact number(s):	010 023 5200
Fax number E-mail address:	popiacompliance@inforegulator.org.za
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	Mr. Darren Epstein (The Information Officer) Dis-Chem Pharmacies Limited
Residential, postal or business address:	Cnr. Le Roux Avenue & Stag Road
	Glen Austin AH
	Midrand
	1685
Contact number(s):	011 589 2200
Fax number/ E-mail address:	darren.epstein@dischem.co.za

A. Please take note that the Information Regulator (Regulator) after having conducted an own initiative assessment in terms of section 89(1) of POPIA, has determined that the responsible party has interfered with the protection of personal information of the data subjects as follows:

X	A breach of the conditions for the lawful processing of personal information.
X	Non-compliance with the duty to notify security compromises (section 22 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with the duty of confidentiality (section 54 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations for direct marketing by means of unsolicited electronic communications (section 69 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding the inclusion of personal information in directories (section 70 of Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding automated decision making (section 71 of the Protection of personal Information Act 4 of 2013)
	Non-compliance with obligations regarding personal information outside the (section 72 of the Protection of Personal Information Act 4 of 2013)
	Breach of the provision of a code of conduct issued in terms of section 60: Code of Conduct ……. of (Reference)

A. BREACH OF THE CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

The responsible party has breached the condition for the lawful processing of personal information listed in the following sections of POPIA:

1. **Section 19 (1)** provides that a responsible party must secure the integrity and confidentiality of personal information under its control or in its possession by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information, and unlawful access to, or processing of personal information.

1.1. **Dis-Chem Pharmacies Limited has violated section 19(1)(b) of POPIA by failing to:**

1.1.1. comply with the provisions of **section 19(1)(b) of POPIA** in that it did not prevent the **unlawful access to or processing of personal information, and by that very fact,** failed to prevent the use of weak passwords. The weak passwords created the breach of confidentiality of personal information due to a brute force attack to compromise the weak passwords, thereby allowing the unlawful access to personal information.

1.1.2. put in place adequate measures to monitor and detect unlawful access to their environment, and failed to ensure that Grapevine, the operator, given the responsibility of processing personal information on its behalf of the data subjects, has adequate security measures in place to secure the integrity and confidentiality of personal information in its possession.

2. **Section 19(2)** provides that a responsible party must take reasonable measures to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

2.1. **Dis-Chem Pharmacies Limited has violated section 19(2) of POPIA by failing to:**

2.1.1. take reasonable measures to **identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control**, and as such, could not identify the risk of using weak passwords, which resulted in a successful brute-force attacks on Dis-Chem and or its operator, Grapevine.

2.1.2. **establish and maintain appropriate safeguards against the risks identified** by not implementing the use of strong and/or complex passwords as a mitigation measure for the identified risk.

2.1.3. **regularly verify that security safeguards against foreseeable risks,** *such as* weak passwords which could result in unlawful access of personal information are adequately implemented.

2.1.4. **ensure that the safeguards are continually updated in response to new risks, or deficiencies in previously implemented security safeguards**, by not concluding an operator agreement with Grapevine as contemplated in section 21(1) of POPIA would ensure that Grapevine which processes personal information for Dis-Chem establishes and maintains measures to secure the integrity and confidentiality of personal information.

3. **Section 19(3)** provides that a responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

3.1. Dis-Chem failed to comply with the provisions of section 19(3) in that:

3.1.1. it did not have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations, by not ensuring adequate access management controls on the environment contrary to the standard of the Payment Card Industry Data Security Standards (PCIDSS). Implementing PCIDSS includes but is not limited to maintaining a vulnerability management programme,

implementing strong access control measures and maintaining an Information Security Policy.

3.1.2. the environment that was affected by the brute force attack was not included in the protection measures that were implemented to safeguard the personal information of data subjects in its possession.

4. **Section 21** provides that a written contract between the responsible party and the operator be entered into, to ensure that the operator that processes personal information for the responsible party establishes and maintains the security measures referred to in section 19 of POPIA.

4.1. **Dis-Chem Pharmacies Limited has violated section 21(1) of POPIA in that:**

4.1.1. it did not conclude a written contract with its operator, Grapevine. The absence of a written agreement between Dis-Chem and Grapevine which would have documented the responsibility of Grapevine in terms of section 21(2) of POPIA resulted in Grapevine failing to notify Dis-Chem of the security compromise.

B. NON-COMPLIANCE WITH THE DUTY TO NOTIFY SECURITY COMPROMISES IN TERMS OF SECTION 22 OF POPIA

5. **Section 22** provides that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, a responsible party must notify the Regulator and the data subject, unless the identity of such data subject cannot be established.

5.1. **Dis-Chem Pharmacies Limited has violated section 22(1) (b)of POPIA in that:**

5.1.1. it did not notify the data subject of the security compromise in terms of section 22(1) (b) as soon as was reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures that were reasonably necessary to determine the scope of the compromise and to restore the integrity of the Dis-Chem's information system.

C. THE INFORMATION REGULATOR MAKES THE FOLLOWING ORDER:

Having regard to the reasons stated herein above and documentation provided by Dis-Chem is ordered to take the following steps:

1. **In respect of the breach of section 19(1):**

1.1. Dis-Chem must 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.

1.2. Dis-Chem must develop and put in place security measures to ensure that the integrity and confidentiality of personal information in its possession or under its control is secured from loss of, damage to, unauthorised destruction or unlawful access to the personal information as it is required by section 19(1) of POPIA.

1.3. Dis-Chem should ensure that the appropriate security safeguards that are put in place include, but are not limited to, the implementation of an adequate Incident Response Plan. The plan must address the following:

1.3.1. Preparation and Prevention,
1.3.2. Detection and Analysis,
1.3.3. Containment and Eradication, and,
1.3.4. Recovery and Post Incident Activities.

2. **In respect of the breach of section 19(2):**

2.1. Dis-Chem must comply with section 19(2) of POPIA by taking reasonable measures to identify all foreseeable internal and external risks to personal information in its possession or under its control.

2.2. Establish and maintain appropriate safeguards against the risks identified, regularly verify that the safeguards are effectively implemented; and ensure that they are continually updated in response to new risks or deficiencies.

3. **In respect of the breach of section 19(3):**

3.1. Dis-Chem must implement PCIDSS by maintaining a vulnerability management programme, implement strong access control measures and maintain an Information Security Policy.

3.2. Ensure that an appropriate Incident Response Plan that makes provision for all aspects of POPIA, Cyber Crimes Act and other related legislative frameworks applicable to the protection of personal information is developed.

3.3. Have due regard to generally accepted information security procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

4. **In respect of the breach of section 21**

4.1. Dis-Chem must 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.

5. **In respect of the breach of section 22**

5.1. Dis-Chem must 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.

D. TIME PERIODS

Dis-Chem must provide a report to the Regulator on the implementation of the recommendations listed in part B, paragraph 1–5 of this notice within thirty-one (31) days of receipt of this notice.

E. RIGHT OF APPEAL

The responsible party may appeal against this Enforcement Notice within thirty (30) working days of receiving this notice.

F. CONSEQUENCES FOR NON-COMPLIANCE WITH AN ENFORCEMENT NOTICE

Please note that a responsible party which fails to comply with this Enforcement Notice is guilty of an offence and liable upon conviction to fine or to imprisonment for a period not exceeding ten (10) years or to both such a fine and such imprisonment.

DATED at **JOHANNESBURG** on this the **31st** day of **August** 2023.

.....

ADV. PANSY TLAKULA

CHAIRPERSON: INFORMATION REGULATOR