INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

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: Department of Justice and Constitutional Development Assessment Report

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject/complainant/aggrieved party:	Own initiative Assessment in terms of section 89 (1) of the Protection of Personal Information Act 4 of 2013 (POPIA)
Unique Identifier/ Identity Number	
Residential, postal or business address:	JD House 27 Stiemens Street Braamfontein Code (2001)
Contact number(s):	
Fax number E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	Director General Adv. Doctor Mashabane The Director General Department of Justice and Constitutional Development
Residential, postal or business address:	Department of Justice and Constitutional Development (DoJ & CD) SALU Building 316 Cnr. Thabo Sehume and Francis Baard Streets Pretoria Code (0001)
Contact number(s):	
Fax number/ E-mail address:	DocMashabane@justice.gov.za

A. Take notice that the Information Regulator (Regulator) after having conducted an own initiative assessment in terms of section 89 (1) of Protection of Personal Information Act 4 of 2013 (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 Republic of South Africa (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)

1. The responsible party has breached the following sections of POPIA:

1.1 **Section 19 (1):** This section requires a responsible party to secure the integrity and confidentiality of personal information in its possession or under its control 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.

1.1.1 The DoJ & CD has violated section 19(1)(a) of POPIA by failing to:

1.1.1.1 put in place adequate technical measures to monitor and detect unauthorised exfiltration (covert outward movement) of data from their environment resulting in the loss of approximately one thousand two hundred and four (1204) files. This stems from the failure of the DoJ & CD to renew the SIEM licenses, which expired in 2020. These licenses are required to enable the DoJ & CD to monitor unusual activity on the network and keep a back-up of the log files. This further resulted in the unavailability of critical information contained within the log files. The DoJ & CD could not keep the backup of these log files due to space limitations on their storage servers.

1.1.1.2 renew the license for the Intrusion Detection System which expired in 2020. This system could have alerted relevant personnel of suspicious activity by unauthorised persons accessing the network.

1.1.1.3 renew the license for the Trend Antivirus which expired in 2020. This failure resulted in the virus definitions for known malware threats not being updated. Ransomware is a type of malicious software that converts files into an unreadable format, essentially causing damage to the information that is contained in those files.

1.1.2 The DoJ & CD has violated section 19(1)(b) of POPIA by failing to:

1.1.2.1 put in place adequate access control measures to prevent the threat actor from gaining access to approximately one thousand, two hundred and four (1204) files.

1.1.2.2 prevent the unauthorised access that enabled the installation of malicious software in the form of the “Mespinoza Ransomware Virus” by an unknown threat actor onto the computer processing infrastructure of the DoJ & CD.

1.2 **Section 19(2):** This section requires a responsible party to 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.

1.2.1 **The DoJ & CD has violated section 19(2) by failing to:**

1.2.1.1 identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control in that it failed to identify the widely known risk of ransomware attacks and or malicious software being deployed on their systems.

1.2.1.2 establish and maintain appropriate safeguards against the risks identified by failing to license the antivirus software, update the Security Incident and Event Monitoring license (SIEM), and update the Intrusion Detection System license.

1.2.1.3 regularly verifying that the security safeguards against malware threats are effectively implemented in that it failed to license the antivirus software more than a year after the license was known to have expired. This meant that there was no protection against a known and detectable virus (Mespinoza ransomware).

1.2.1.4 ensure that the safeguards are continually updated in response to new risks, or deficiencies in previously implemented security safeguards in that it failed to continually ensure that the security safeguards which prevent malicious software deployment are updated to respond to new risks that may have manifested as a result of the continued use of unlicensed software.

1.3 **Section 19(3):** This section 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.

1.3.1 **The DoJ & CD has violated section 19(3) by failing to:**

1.3.1.1 have an updated Incident Response Plan in place which incorporates the applicable provisions of section 22(1) of POPIA. The International Organisation for Standardisation (ISO) on Cyber Security, specifically, A.16.1.5 of ISO 27001 requires that an Incident Response Plan should define how information security weaknesses will be dealt with and be continuously updated.

1.4 **Section 22(1):** This section provides that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unreasonable person, a responsible party must notify the Regulator and the data subject, unless the identity of such data subject cannot be established.

1.4.1 **The DoJ & CD has violated section 22(1) by failing to:**

1.4.1.1 update the Incident Response Plan which could have enabled it to notify the Regulator and the data subject of the security compromise as soon as reasonably possible after it was discovered. The Regulator was only notified of the security compromise after it requested the DoJ & CD to do so. Whilst the Regulator accepts that the identity of the data subjects who were affected by the security compromise could not be established due to

the encryption of the data on the compromised processing environment, the affected data subjects could still have been notified of the security compromise by publishing a general notice in the media.

B. The DoJ & CD is hereby ordered to:

Take the following specified steps:

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

1.1 Provide the Regulator with copies of the Personal Information Impact Assessment (PIIA) and the Compliance Framework in terms of Regulation 4(1)(a) of POPIA within thirty-one (31) days of receipt of this Notice.

1.2 Report the security compromise to the South African Police Service (SAPS) and submit proof thereof to the Regulator within thirty-one (31) days of receipt of this Notice.

1.3 Submit proof to the Regulator within thirty-one (31) days of receipt of this Notice that the Anti-Virus software, the SIEM license and the Intrusion Detection System have been renewed.

1.4 Institute disciplinary proceedings against the official(s) who are responsible for the renewal of the licenses mentioned in paragraph 1.3 above and submit proof thereof to the Regulator within thirty-one (31) days of receipt of this Notice.

1.5 Provide training on POPIA to all staff. The training manual should be submitted to the Regulator within thirty-one (31) days of receipt of this Notice.

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

2.1. Provide proof that reasonable measures have been taken to identify all foreseeable internal and external risks to personal information in its possession or under its control, establishes 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 it previously implemented within thirty-one (31) of receipt of this Notice.

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

3.1. Update the Incident Response Plan by incorporating all applicable provisions of POPIA and provide proof thereof to the Regulator within thirty-one (31) days of receipt of this Notice.

3.2. Implement the Public Service Corporate Governance of Information and Communication Technology Framework, dated December 2012 and provide proof thereof to the Regulator within thirty-one (31) days of receipt of this Notice.

4. In respect of the breach of section 22(1)

4.1. Ensure that the Compliance Framework for POPIA and the Incident Response Plan referred to in paragraph 1.1 and 3.1 is developed and implemented within thirty-one (31) days of receipt of this Notice.

C. Right of Appeal

The responsible party may appeal against this Enforcement Notice within thirty (30) days of the date of receipt of this Enforcement Notice as provided for in section 97(1) of POPIA.

D. 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 09**th** day of **May** 2023

……

ADV. PANSY TLAKULA

CHAIRPERSON OF THE INFORMATION REGULATOR