INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

MEDIA STATEMENT

ENFORCEMENT NOTICE ISSUED TO THE DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT DUE TO CONTRAVENTION OF POPIA

10 MAY 2023

On 9 May 2023 the Information Regulator (Regulator) issued an Enforcement Notice to the Department of Justice and Constitutional Development (DoJ&CD) following the finding of the contravention of various sections of the Protection of Personal Information Act (POPIA) by the DoJ&CD.

In September 2021 the DoJ&CD suffered a security compromise on its IT systems. This led to the department's systems being unavailable to its employees and subsequently affecting services to the public. The Regulator conducted an own initiative assessment after the Department suffered a security compromise (data breach).

Following the assessment, the Regulator found that the department had failed to put in place adequate technical measures to monitor and detect unauthorised exfiltration of data from their environment resulting in the loss of approximately 1204 files. This occurred as a result of the DoJ&CD's failure to renew the Security Incident and Event Monitoring (SIEM) licence which would have enabled it to monitor unusual activity on their network and keep a backup of the log files. The failure to renew the licence resulted in the unavailability of critical information contained in the log files. The SIEM licence expired in 2020.

The DoJ&CD also failed to renew the Intrusion Detection System licence, which had also expired in 2020. Had this licence been renewed, the department would have received alerts of suspicious activity by unauthorised people accessing the network. The Trend Antivirus licence was also not renewed in 2020 when it expired. The failure to renew this licence resulted in the virus definition for known malware threats not being updated.

The Regulator also found that the DoJ&CD had failed to take reasonable measures to identify or reasonably foreseeable internal and external risks to the protection of personal information in its possession or under its control and establish and maintain appropriate safeguards

against the identified risks. In this regard, the department failed to establish and maintain appropriate safeguards against the risks identified and to regularly verify and update the security safeguards against malware threats.

Following the finding that the DoJ&CD had contravened section 19 and 22 of POPIA, the Regulator issued the DoJ&CD with an Enforcement Notice in which it orders the department to take a number of steps. These steps include that the department must submit proof to the Regulator within 31 days of receipt of the Notice that the Trend Anti-Virus licence, the SIEM licence and the Intrusion Detection System licence have been renewed. It must also institute disciplinary proceedings against the official/s who failed to renew the licences which are necessary to safeguard the department against security compromises. Should the DoJ&CD fail to abide by the Enforcement Notice within the stipulated timeframe, it will be guilty of an offence, in terms of which the Regulator may impose an administrative fine in the amount not exceeding R10 million, or liable upon conviction to a fine or to imprisonment of the responsible officials.

With the rising scourge of security compromises, responsible parties are urged to improve their information security systems to ensure that there are adequate safeguards to protect personal information of data subjects in their possession or under their control. The Regulator places emphasis on the management of risks arising from security compromises.

For media enquiries, contact Ms Nomzamo Zondi at 078 674 2598 or Nzondi@inforegulator.org.za.

ISSUED BY THE INFORMATION REGULATOR OF SOUTH AFRICA.