MEDIA STATEMENT

INFORMATION REGULATOR'S IT SYSTEMS AFFECTED BY A RANSOMWARE ATTACK ON THE DEPARTMENT OF JUSTICE & CONSTITUTIONAL DEVELOPMENT

13 SEPTEMBER 2021

The Information Regulator notes with concern media reports and an official public statement from the Department of Justice and Constitutional Development (DOJ&CD), released on 09 September 2021, that its Information Technology (IT) systems suffered a security breach that was caused by a ransomware attack. The breach took place on the evening of 06 September 2021.

Even more concerning is that this security breach did not only interrupt the DOJ&CD's IT systems, but also impacted on the work of the Information Regulator which relies on the DOJ&CD's IT systems for its own operations. As a result of this security breach the Regulator's website (https://www.justice.gov.za/inforeg/) was temporarily unavailable (for three days), and the e-mail system went offline and remains unavailable.

The Regulator has written to DOJ&CD to remind them of their obligations in terms of Section 22 of POPIA which requires responsible parties to notify the Regulator and the data subject where reasonable grounds exist and the personal information of a data subject has been accessed or acquired unlawfully. One of the matters which the Regulator has sought details on from the DOJ&CD is the impact of the security breach on information systems of the Department and its stakeholders.

The chairperson of the Regulator, Advocate Pansy Tlakula, has expressed her concern with the security breach. "It is very unfortunate that this breach has occurred. As the Regulator we are concerned about the high number of security breaches in South Africa. In August alone, thirty-eight (38) responsible parties suffered, and reported, security breaches. Responsible parties are reminded of their obligation under POPIA to secure the integrity and confidentiality of personal information of data subjects by taking appropriate, reasonable technical and

organisational measures to prevent unlawful access to or processing of personal information. It is our role to ensure that personal information is processed safely and securely. Failure to do so has legal consequences," she said.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge. This has led to all the information systems being encrypted and unavailable to both internal employees as well as members of the public. As a result, all electronic services provided by the Regulator have been affected, including emails, applications, complaints and the website.

The Regulator would like to once again assure the stakeholders that the IT teams are working around the clock to restore services as soon as possible. So far no indication of data compromise has been detected on the systems. The Regulator apologises for the inconvenience caused.

For media enquiries contact:

Tshegofatso Letshwiti

073 648 9857

Tletshwiti.IR@gmail.com

ISSUED BY THE INFORMATION REGULATOR OF SOUTH AFRICA