INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Address: JD House, 27 Stiemens Street
Braamfontein, Johannesburg, 2001
P.O. Box 31533
Braamfontein, Johannesburg, 2017
Tel: 010 023 5200
Email: enquiries@inforegulator.org.za

To: All the Data Subjects of the Information Regulator;

Dear All,

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 (POPIA)

1. In terms of section 22 of the Protection of Personal Information Act No. 4 of 2013 (POPIA), where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator (Regulator) and the data subject, unless the identity of such data subject cannot be established.

2. POPIA defines a data subject as a person to whom personal information relates, and the responsible party is defined as a public or private body which determines the purpose of and means for processing personal information. Therefore any person that has, in the course of interacting with the Regulator, submitted their personal information to the Regulator, that person is a data subject of the Regulator in terms of POPIA.

3. It is in that respect that the Regulator wishes to notify potentially affected persons who are 'data subjects' of the Regulator about the malware that attacked the Information Technology (IT) systems of the Department of Justice and Constitutional Development (DoJ&CD) as was confirmed by the DoJ&CD in a public statement on 09 September 2021.

4. The Regulator, as a new entity, has been relying on the IT systems of the DoJ&CD from the date of its inception up until now. In terms of the transitional arrangements with the DoJ&CD, the Regulator is a responsible party and the DoJ&CD is an Operator, as defined in the POPIA. Therefore, as a responsible party the Regulator has an obligation to notify its data subjects about the security breach.

5. As a responsible party, the Regulator was assured that the DoJ&CD has the following seven layers of data protection that are in compliance with section 19 of POPIA-

2.1 Access Control;
2.2 Data Encryption;
2.3 Defensive Measures;
2.4 Robust Monitoring, Auditing and Reporting capabilities;
2.5 Data Backups;
2.6 Anti-virus and Anti-malware Solutions; and
2.7 Awareness and Vigilance

6. The Regulator has, in accordance with section 22(1) of the POPIA and despite the above-mentioned security measures in place, reasonable grounds to believe that your personal information may have been accessed or acquired by an unauthorised person, and below is the information currently available to allow you to take protective measures against the potential consequences of the compromise-

6.1 Brief description of incident and the number of data subject(s) whose personal information has been compromised.

6.1.1 On or about 9th September 2021 and through the media statement from the DoJ&CD, the Regulator became aware of the security compromise on the IT Systems of the DoJ&CD, in terms of which the DoJ&CD advised that the aforesaid security compromise was effected through ransomware on the evening of 6 September 2021. The DoJ&CD advised that ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading which occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

6.1.2 The DoJ&CD further advised that the security compromise has led to all IT systems of the DoJ&CD being encrypted and unavailable to both internal employees as well as members of the public.

6.1.3 In subsequent correspondence from the DoJ&CD (dated 20 September 2021) the Regulator was informed that the issue was detected within the Citrix environment (where applications are hosted) whereby connectivity was lost between application and database servers on the evening of 05 September 2021. As a result all user accounts on the Active Directory were locked. The analysis that was done therefore concluded that it was a malware infection, suspected to be ransomware.

6.1.4 The DoJ&CD has indicated that the Security Incident Analysis report shows that the breach occurred as a result of one of the domain administrator accounts being compromised and used to deploy ransomware in the DoJ&CD's ICT environment.

6.1.5 As a result, the DoJ&CD has confirmed to the Regulator that there was unauthorised access to its ICT systems and that data was accessed and sent outside the DoJ&CD. It has not yet been established if that data included the Regulator's data and that of its data subjects.

6.1.6 The Regulator assures all affected parties that its IT teams are working tirelessly in collaboration with the DoJ&CD, to restore services as soon as is practically possible and minimise the potential consequences of the compromise.

6.2 The date of the security Compromise, or if unknown

The Regulator was advised by the DoJ&CD that the security compromise was effected through ransomware on the evening of 5 September 2021.

6.3 The identity of the unauthorised person who may have accessed or acquired the personal information.

The Regulator is currently not aware of the identity of the unauthorised person who may have accessed or acquired your personal information and investigation is currently underway.

The DoJ&CD has informed the Regulator that even though the identity of person that had unauthorised access is not known, the investigation has led to the discovery of text files that are consistent with ransomware, those files contain instructions to the Department to contact what seems to be the perpetrators. However the DoJ&CD has advised that no demand for money has been made as at 20 September 2021.

6.4 The categories of personal information that may have been accessed or acquired unauthorised person

The DoJ&CD has indicated in its report to the Regulator that at this stage the investigations are inconclusive in terms of the exact nature of the information that was sent outside the ICT systems of the DoJ&CD. Therefore, the types of personal information of its data subjects that may have been compromised is not yet determined. However the DoJ&CD's Security Incident Analysis report has indicated that at least

1200 files were exfiltrated. According to the DoJ&CD these flies may have contained personal information such as addresses and bank account details. In addition to that, it is the view of the Regulator that these files may have contained your personal information, such as:

6.4.1 Names, addresses, Identity Numbers, Phone numbers of information officers;

6.4.2 Names, residential addresses, Identity Numbers, Phone numbers, qualifications, bank accounts and salaries of employees; and

6.4.3 Names, addresses and bank details of the service providers.

6.5 Whether the notice was delayed as a result of a law enforcement investigation.

The Regulator became aware of the possible security compromise through a media statement on 9 September 2021 and was officially notified on 13 September 2021, after having sent correspondence to the DoJ&CD reminding the department of the their obligation notify the Regulator and data subjects in accordance with section 22 of POPIA.

6.6 Description of the possible consequences of the security compromise

The possible consequences is the selling of the personal information and fraud being committed using the compromised, if any, personal information.

6.7 Description of the measures that the Regulator intends to take or has taken to address the security compromise and to protect the personal information of the data subjects from further unauthorised access or use.

6.7.1 In so far as the data of the Regulator still being held by the DOJ&CD is concerned, the DoJ&CD has advised the Regulator that its IT Systems are, as part of measures taken to address the security compromise and to protect the personal information of the data subjects from further unauthorised access or use**,** protected by the following features-

6.7.1.1 Access Control by way of strong password enforcement, Privileged Access Manager (PAM), and Virtual Private Network (VPN) access;

6.7.1.2 Defensive Measures, Including Third Party Firewalls, and Intrusion Prevention System (IPS), Security Event And Incident Monitoring (SEIM);

6.7.1.3 Anti-virus and Anti-malware Solutions on both server infrastructure and end-points.

6.7.2 The DoJ&CD has further advised the Regulator that it has put in place the following preventative measures-

6.7.2.1 Implemented monitoring tools (QRadar) to assist in ensuring any suspicious activity can be detected and deals;

6.7.2.2 Installed Deep Discovery and Deed Security on critical servers, which provide better protection;

6.7.2.3 Continuously initiating campaigns to staff on ICT security awareness;

6.7.2.4 Active Directory hardening, with assistance from Microsoft Rapid Recovery team, will ensure that a new Active Directory forest be built that is clean, and without any compromise.

6.7.3 As for the Regulator, it has established its own email system and has put security controls in place with measures such as identify protection, anti-malware protection, multi-factor authentication, device management, threat protection and encryption. All these security measures will ensure that personal information of data subjects is protected and secured.

6.7.4 The Regulator is developing an Information Officer Registration Portal that will be hosted on the cloud service fortified with two-factor authentication, encryption, next generation firewalls to detect and prevent intrusion and patch management.

6.7.5 The Regulator is in the process of implementing its own website to establish and maintain with its security controls such as firewalls, patch management, monitoring and access control.

6.7.6 The Regulator is in constant communication with DoJ&CD in establishing how the assessment of the IT environment and systems are progressing.

6.7.7 The Regulator will be commencing its own independent investigation into the security breach and the impact it has had on personal information of its data subjects.

6.8 Advice or recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise.

6.8.1 The Regulator advises that-

6.8.1.1 you remain vigilant by reviewing your account statements; and

6.8.1.2 you immediately contact the law enforcement in the event of actual or suspected identity theft.

7. **Contact information of the Regulator should the data subject require any further assistance**

Contact information of the Regulator is as follows-

Physical address:	JD House 27 Stiemens Street Braamfontein Johannesburg 2001
Postal Address:	P.O Box 31533 Braamfontein, Johannesburg 2017
Tel:	+27 (0) 10 023 5200,
Email:	enquiries@inforegulator.org.za

8. For further information and assistance, please contact Ms Deborah Lamola at enquiries@inforegulator.org.za or visit *https://www.justice.gov.za/inforeg/*.

Adv. P. Tlakula
Chairperson: Information Regulator
Date: 22 September 2021