TECHNOLOGY &
COMMUNICATIONS SECTOR

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

If it happened to them, it could happen to you: Lessons from the Information Regulator

Compiled by Preeta Bhagattjee, Aphindile Govuza and Jessica van den Berg

11 OCTOBER 2021

A business' operations can be brought to a standstill if it experiences a data breach – a reality which is becoming more and more familiar. Section 22 of the Protection of Personal Information Act 4 of 2013 (POPIA) requires responsible parties to notify both the Information Regulator and the relevant data subject(s) of a breach where there are reasonable grounds to believe that their personal information has been accessed or acquired by any unauthorised person. The Information Regulator itself recently had the unfortunate opportunity to demonstrate this requirement.

On or about 9 September 2021, the Information Regulator became aware of a security compromise at the Department of Justice and Constitutional Development (DoJ&CD), whose information and communication technology (ICT) systems the Information Regulator shares. The DoJ&CD have advised that the security compromise was effected through ransomware on its systems on 6 September 2021. The DoJ&CD further confirmed that there was unauthorised access to its ICT systems, and as a result, one of the domain administrator's accounts was compromised and used to deploy ransomware in the DoJ&CD's ICT environment.

As is required in terms of section 22 of POPIA, on 22 September 2021, the Information Regulator issued a notification of security compromise (Notice) to all its data subjects (whom the Information Regulator identifies as *"any person that has, in the course of interacting with the [Information] Regulator, submitted their personal information to the [Information] Regulator"*). A copy of the Notice was published on the Information Regulator's website. The Notice covers the following key points:

- the identity of the unauthorised person who may have accessed or acquired the personal information;
- the categories of personal information that may have been accessed or acquired by the unauthorised person;
- a description of the possible consequences of the security compromise;
- a description of the measures that the Information 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; and
- advice or recommendations with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise.

Any person who is a data subject, as described in the notice, should take protective measures against the compromise to protect themselves.

Proactive approach

Through the Notice, the Information Regulator has demonstrated a proactive approach to data breaches, in that although it is currently still making use of the DOJ&CD's ICT systems, it is also taking its own steps as a responsible party to strengthen its security measures and ensure the protection of personal information of data subjects in the future.

These measures include establishing its own email system with security controls in place; ensuring that cloud service hosting options for its Information Officer Registration Portal are fortified with two-factor authentication, encryption and next generation firewalls; implementing its own website; and, importantly, commencing its own independent investigation into the security breach and any impact on the personal information of its data subjects.

Data breaches can have devastating effects on targeted businesses and businesses should prepare for such eventualities by implementing appropriate, reasonable technical and organisational measures to prevent the loss of, damage to, or unauthorised destruction of personal information and unlawful access to or processing of personal information, in accordance with POPIA. In addition to implementing such measures, and in order to deal with breaches swiftly when they do happen, businesses should also proactively develop and implement (throughout the business) a POPIA-compliant data breach response plan.

Furthermore, we note that the Information Regulator is expected to publish a template for responsible parties to use in order to notify the Information Regulator of such a breach – a development which is most welcome.