CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

13 JULY 2023

Corporate & White Collar Investigations

ALERT

IN THIS ISSUE

Protection of Personal Information Act (POPIA)

On 3 July 2023, the Information Regulator issued the first administrative fine for POPIA violations and failure to comply with an enforcement notice. This alert considers the key lessons that can be drawn from the fact that the Department of Justice and Constitutional Development failed to remedy the information security shortcomings identified by the Information Regulator and is now the first responsible party to be sanctioned for non-compliance.

FOR MORE INSIGHT INTO OUR EXPERTISE AND SERVICES

Protection of Personal Information Act (POPIA)

On 3 July 2023, the Information Regulator issued the first administrative fine for POPIA violations and failure to comply with an enforcement notice. This alert considers the key lessons that can be drawn from the fact that the Department of Justice and Constitutional Development failed to remedy the information security shortcomings identified by the Information Regulator and is now the first responsible party to be sanctioned for non-compliance.

Don't ignore an enforcement notice: The Information Regulator issues the first fine for a POPIA contravention

After receiving over 500 notifications of personal information violations and facing criticism for failing to act on reports made by data subjects, the Information Regulator issued an infringement notice and its first administrative fine on 3 July 2023.

In May 2023, the Information Regulator found that the Department of Justice and Constitutional Development (DoJ&CD) had contravened section 19 and 22 of the Protection of Personal Information Act 4 of 2013 (POPIA) based on data breaches in its IT environment in September 2021. Approximately 1,204 files that contained personal information were lost. After an assessment, the Information Regulator found that the department had failed to renew its security incident and event monitoring, intrusion detection system and Trend antivirus licences which had expired in 2020, and which would have alerted the department to the attempts to access the network had the services been active. Failure to have the required security in place resulted in unauthorised access to the network and the compromising of personal information due to inadequate protection measures.

The Information Regulator then issued an enforcement notice which gave the DoJ&CD opportunity to remedy the shortcomings, discipline the relevant officials and submit proof thereof to the Information Regulator within 31 days. Despite being issued with the notice, the department failed to take the necessary corrective steps and did not submit proof that the issues had been remediated as stipulated before expiry of the notice on 9 June 2023. In fact, the DoJ&CD did not communicate with the Information Regulator. It has now been fined R5 million for failure to

Protection of Personal Information Act (POPIA)

CONTINUED

comply with the enforcement notice. The department has 30 days from 3 July 2023 to pay the administrative fine, make arrangements with the regulator to pay the administrative fine in instalments, or elect to be tried in court on a charge of having committed an offence in terms of POPIA.

There are lessons for natural and juristic persons to learn from the failures of the DoJ&CD and from the response of the Information Regulator, which has confirmed that there going to be more penalties and administrative fines issued for violations of POPIA.

Personal information must be kept secure

Condition 7 of POPIA, which is part of *"Processing of personal information in general"*, expounds on the personal information security safeguards that responsible parties have to implement. In section 19, it is stated that:

> *"Security measures on integrity and confidentiality of personal information*
>
> *(1) A responsible party must 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:*
>
> *(a) loss of, damage to or unauthorised destruction of personal information; and*
>
> *(b) unlawful access to or processing of personal information.*
>
> *(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to:*
>
> *(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;*
>
> *(b) establish and maintain appropriate safeguards against the risks identified;*
>
> *(c) regularly verify that the safeguards are effectively implemented; and*
>
> *(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards."*

Responsible parties are expected to adhere to accepted information security standards as dictated by the environment and the type of information that must be protected. A risk-based approach is required to identify and measure the adverse

Protection of Personal Information Act (POPIA)

CONTINUED

activities that could compromise the information that is held by the responsible party. The mitigating actions taken by the responsible party must be appropriate and demonstrable. This will include governance frameworks, technological measures such as security software, the physical securing of data and the requisite employee skills for effective information protection.

The DOJ&CD was found to have acted negligently by failing to ensure that licenses for security software had been renewed and the information in its environment was secure by managing the risk of unauthorised access with adequate control measures. The Information Regulator also stated that the officials who were responsible for ensuring that the correct measures were in place had to be disciplined for their lack of action.

The onus rests on organisations to ensure that the personal information they collect, process and store is secure at all times and not at risk of unauthorised access, misuse or loss. This can be achieved by:

- implementing and maintaining the required effective frameworks, physical and technological safeguards;
- ensuring that officials who are responsible for protecting information have the required skills and tools to achieve security objectives; and
- conducting regular risk assessments to measure the effectiveness of protection measures against current and novel threats.

Notify the Information Regulator if security is compromised or a data breach occurs

If a security compromise, data breach or any unauthorised access of personal information occurs, according to section 22 of POPIA, the responsible party must notify:

- the Information Regulator; and
- the data subject, unless the identity of such data subject cannot be established.

Notifying the Information Regulator is a legislated requirement that is not optional for responsible parties. The responsible party must notify the regulator as soon as reasonably possible after the incident. The Chairperson of the Information Regulator, Adv. Pansy Tlakula,

Protection of Personal Information Act (POPIA)

CONTINUED

previously stated that all security compromises must be reported, even if the personal information of only one person is involved. The Information Regulator has published the *"Guidelines on Section 22 Notification of Security Compromises or Guidelines on Completing Section 22 Security Compromise Notification Form"* document which details the process that must be followed for making a report when a data breach occurs. Organisations can access the guidelines online and must follow the clearly defined steps for reporting security compromises.

In this matter, the DoJ&CD failed to report the security compromise to the Information Regulator after it occurred, and the Information Regulator instituted an assessment of the data breach on its own initiative. Serious shortcomings in information security were identified and detailed feedback was provided to the DoJ&CD in the form of an enforcement notice.

Comply with an enforcement notice

An enforcement notice is a statement issued by the Information Regulator stipulating the corrective actions which must be undertaken by a responsible party to rectify shortcomings in the protection of personal information which result in non-compliance with POPIA.

The legislation states that if a responsible party is deemed to have failed to comply with the requirements of POPIA, the Information Regulator may, according to section 95,

> *"(1) serve the responsible party with an enforcement notice requiring the responsible party to do either or both of the following:*
>
> *(a) to take specified steps within a period specified in the notice, or to refrain from taking such steps; or*
>
> *(b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice."*

A responsible party can elect to appeal against an enforcement notice by application to the High Court, or to comply with it. It is our considered view that, unless the responsible party is absolutely certain that the Information Regulator has erred in issuing the enforcement notice, it is best to comply with the notice and undertake remedial action as recommended by the Information Regulator. Organisations must take cognisance of the fact that failure to comply with an enforcement notice is a serious offence which can result in imprisonment for a period not exceeding 10 years or a fine not exceeding R10 million or both.

Protection of Personal Information Act (POPIA)

CONTINUED

After being issued with an enforcement notice in May 2023, the DOJ&CD was given 31 days to comply with the requirements of the notice, but it failed to do this and, as a result, it was then issued with an infringement notice and an administrative fine of R5 million. Not only did the department fail to protect the personal information of data subjects, but it has also caused itself reputational and financial harm by becoming the first entity to be sanctioned under POPIA. It had the opportunity to address the areas of deficiency as provided by the Information Regulator but did not do so.

In conclusion, the Information Regulator has shown that it will act against violations of personal information. It is ironic that the first infringement notice and administrative fine were issued against the DOJ&CD, which is expected to be in forefront of understanding the importance of compliance with the law. This failure by the department should serve as a warning for organisations that are not POPIA compliant, and which do not take violations of the protection of personal information seriously, to act immediately and ensure that they do not become the next party to be sanctioned by the Information Regulator.

Tendai Jangara

OUR TEAM

For more information about our Corporate & White Collar Investigations team and services in South Africa and Kenya, please contact:

Rishaban Moodley
Practice Head & Director:
Dispute Resolution
Sector Head:
Gambling & Regulatory Compliance
T +27 (0)11 562 1666
E rishaban.moodley@cdhlegal.com

Tim Fletcher
Chairperson
Director: Dispute Resolution
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com

Eugene Bester
Director:
Dispute Resolution
T +27 (0)11 562 1173
E eugene.bester@cdhlegal.com

Chris Charter
Practice Head & Director:
Competition Law
T +27 (0)11 562 1053
E chris.charter@cdhlegal.com

Jackwell Feris
Sector Head:
Industrials, Manufacturing & Trade
Director: Dispute Resolution
T +27 (0)11 562 1825
E jackwell.feris@cdhlegal.com

Anja Hofmeyr
Director:
Dispute Resolution
T +27 (0)11 562 1129
E anja.hofmeyr@cdhlegal.com

Tendai Jangara
Director:
Dispute Resolution
T +27 (0)11 562 1136
E tendai.jangara@cdhlegal.com

Corné Lewis
Director:
Dispute Resolution
T +27 (0)11 562 1042
E corne.lewis@cdhlegal.com

Richard Marcus
Director:
Dispute Resolution
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com

Burton Meyer
Director:
Dispute Resolution
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com

Desmond Odhiambo
Partner | Kenya
T +254 731 086 649
T +254 204 409 918
T +254 710 560 114
E desmond.odhiambo@cdhlegal.com

Aadil Patel
Practice Head & Director: Employment Law
Joint Sector Head:
Government & State-Owned Entities
T +27 (0)11 562 1107
E aadil.patel@cdhlegal.com

Lucinde Rhoodie
Director:
Dispute Resolution
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

Belinda Scriba
Director:
Dispute Resolution
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com

Krevania Pillay
Senior Associate:
Dispute Resolution
T +27 (0)11 562 1317
E krevania.pillay@cdhlegal.com

BBBEE STATUS: LEVEL ONE CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa.
Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

NAIROBI
Merchant Square, 3rd floor, Block D, Riverside Drive, Nairobi, Kenya. P.O. Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114
E cdhkenya@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

CLIFFE DEKKER HOFMEYR | cliffedekkerhofmeyr.com

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA