Complying with South Africa's Protection of Personal Information Act

Entrust helps enterprises comply with South Africa's Protection of Personal Information Act

- Secure personal data using a certified, tamper-resistant platform
- Protect legally shared personal data from disclosure
- Prepare and maintain records of personal data processing

SUMMARY

In November, 2013, the Parliament of the Republic of South Africa enacted the Protection of Personal Information Act, 2013 (POPIA):

To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.

LEARN MORE AT ENTRUST.COM/HSM

Potential consequences of non-compliance

Sections 100 – 106 of the POPI Act deal with instances where parties would find themselves "guilty of an offence". Specifically, **Section 105** (Unlawful Acts by responsible party in connection with account number) states that "the responsible party must…have known or ought to have known that…[a violation of personal data privacy] would likely cause substantial damage or distress to the data subject."

Additionally, **Section 106** (Unlawful Acts by third parties in connection with account number) states that "a person who knowingly or recklessly, without the consent of the responsible party…obtains or discloses an account number of a data subject… or procures the disclosure of an account number of a data subject to another person is…guilty of an offence."

Section 107 details which penalties apply to respective offenses. Specifically, "Any person convicted of an offence…is liable… to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine

1. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Complying with South Africa's Protection of Personal Information Act

and such imprisonment; or …to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment."

As detailed in **Section 109** of the Act, the maximum fine "may not exceed R10 million."

Protection of personal information

The following material is excerpted directly from the Republic of South Africa's POPI Act.

Security measures on integrity and confidentiality of personal information

19. (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.

Security measures regarding information processed by operator

21. (1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

Notification of security compromises

22. (1) 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—

(a) the Regulator; and

(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

…

(4) The notification to a data subject… must be in writing and communicated to the data subject in at least one of the following ways:

a) Mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

Complying with South Africa's Protection of Personal Information Act

Civil remedies

99. (1) A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.

...

(3) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable, including—

(a) payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;
(b) aggravated damages, in a sum determined in the discretion of the Court;
(c) interest; and
(d) costs of suit on such scale as may be determined by the Court.

How Entrust can help you comply with POPIA and avoid the data breach notification requirement

POPIA is unclear about what is considered to be access and acquisition of subject data. Other regulations around the world that deal with protection of personal information state that if the data has been pseudonymised or made unreadable to whomever illegally retrieved it, then the data breach does not need to be reported; the stolen sensitive data has been rendered useless to the thieves and harmless to the data subject.

The two widely accepted best practice approaches to pseudonymisation are encryption and tokenization. Both employ cryptographic keys to convert plain text to unreadable ciphertext and back again. If 'cyberthieves' steal the keys along with the encrypted or tokenized data, they can then convert the data back to plain text. So, it is essential to separate the keys from the data they protect and to provide additional security for the keys themselves.

Entrust solutions for cryptographic key security

Best practice for cryptographic key security is to store those keys in a hardware security module (HSM). Entrust's nShield® HSMs are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. These HSMs are tested, validated and certified to the highest security standards including FIPS 140-2 and Common Criteria. nShield HSMs enable organizations to:

- Meet and exceed established and emerging regulatory standards for data privacy
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com