ENSafrica | Africa's largest law firm **issue 8** | 2020-02

ENSafrica privacy in brief

issue 8 | ENSafrica's newsworthy stories on data privacy and compliance.

newsflash

The commencement date of POPIA is no April Fool's joke

- the Chairperson of the Information Regulator, Advocate Pansy Tlakula, recently sent a request to President Cyril Ramaphosa to declare that the remaining provisions of the Protection of Personal Information Act, 2013 ("**POPIA**") commence on 1 April 2020 ("**commencement date**").
- it is expected that the president will act on this request. A responsible party (ie, a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information) will then be given a one year transitional period after the commencement date to comply with its provisions. That means that organisations will have to be POPIA-compliant by 31 March 2021.
- read the full article here.

feature topic

Sanction screening vs data protection

- in terms of South African legislation, entities should not deal with persons or entities who have been sanctioned by the United Nations Security Council ("**UNSC**")
    - section 25 of the Protection of Constitutional Democracy Against Terrorist and Related Activities, 2004 ("**POCDATARA**") says that the president must give notice that the UNSC has imposed sanctions. Section 4 of POCDATRA expressly prohibits any person from dealing with property that is associated with entities that are sanctioned pursuant to POCDATARA.
    - under section 26A (3) of the Financial Intelligence Centre Act, 2001 ("**FICA**"), the Minister of Finance must announce the adoption of UNSC resolutions for financial sanctions. Thereafter, in terms of section 26B of FICA, a person may not (subject to limited exceptions) deal with a person or an entity who has been sanctioned.
    - section 28A of FICA obliges accountable institutions, such as banks and money remitters, upon the publication of a proclamation under section 25 of POCDATARA or section 26A (3) of FICA as above, to scrutinise their information concerning clients with whom the accountable institution has business relationships in order to determine whether any such client is a person or entity mentioned in the proclamation or the notice. If a positive hit is found, a report must be filed by the accountable institution to the Financial Intelligence Centre.

- the Office of Foreign Assets Control of the United States ("**OFAC**") has previously penalised non-US banks for processing USD transactions involving countries sanctioned for terrorist and related activities.
- because of the significant risks for non-US banks and other companies that do business with OFAC-sanctioned jurisdictions or persons using USD payments, South African entities often perform sanction screening on employees, customers and suppliers that go beyond the requirements of local legislation (ie, FICA and POCDATARA which ban transactions with UNSC-sanctioned entities only).
- however, the legality of these screening operations is questionable under data privacy and protection legislation. While the substantive provisions of POPIA are not yet in force, the EU General Data Protection Regulation 2016/679 ("**GDPR**"), which, in certain instances applies directly to South African entities, came into force on 25 May 2018.
- in terms of section 26 of POPIA, the processing of personal information concerning criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings, as a general rule, is prohibited unless the data subject has consented to such processing.
- in terms of Article 10 of the GDPR, the lawful processing of personal data relating to criminal convictions and offences or related security measures must be carried out only under the control of official authority or be authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.
- processing is therefore permitted if it its origin is in EU sanctions lists.
- on the contrary, the processing of personal data based on US listings does not constitute a legal obligation stemming either from EU law, or from the law of one of the member states.
- in this regard, the medical technology and life sciences multinational, GE Healthcare Group, made an application to the Swedish data protection authority for an exemption for the processing of personal data in order to comply with US (ie, OFAC) sanctions lists. The Swedish Data Protection Authority refused to grant the exemption and the matter was brought before the Administrative Court in Stockholm's county.
- while the court recognised the legitimate interest of the company to comply with the OFAC sanctions, it still found that these considerations were insufficient to offset the fundamental data-protection rights of the individuals concerned.
- it would seem as if the right to data protection and privacy (especially where special personal information is involved) under the GDPR and POPIA cannot, without further safeguards, be overridden by business and other interests in complying with OFAC and other sanctions.
- GDPR penalties for non-compliance may be up to EUR20-million or 4% of the total global turnover of an entity and non-compliance with POPIA (once in force) can lead to imprisonment of up to 10 years or a ZAR10-million fine, or both. However, penalties for US sanctions violations can exceed these amounts.
- to avoid falling foul of POPIA and to prevent sanction violations, it is recommended that entities obtain consent from data subjects in respect of sanction screening. Such consent must be a voluntary, specific and informed expression of will and can,

for example, be included in privacy policies, customer terms of conditions, onboarding forms and the like. ENSafrica can assist in this regard.

POPIA in brief

Condition 8: Data subject participation

- a data subject, having provided adequate proof of identity, has the right to request the organisation to confirm, free of charge, whether the responsible party holds personal information about the data subject; and request the record or a description of this personal information, including information about the identity of all third parties, who have, or have had, access to the information in a form that is generally understandable within a reasonable time and at a prescribed fee.

- a data subject may request a responsible party to correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully about the data subject in its possession or under its control; or destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of POPIA's retention and restriction of records provisions. Regulation 3 of the POPIA Regulations provides that the data subject must submit this request to the responsible party on Form 2.

- the responsible party, or a designated person, must render such reasonable assistance (as is necessary free of charge) to enable a data subject to complete Form 2.

- on receipt of such request, the responsible party must, as soon as reasonably practicable, correct the information; destroy or delete the information; provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

- if the responsible party has taken steps that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps. The responsible party must, in addition, notify the data subject (who has made a request) of the action taken as a result of the request.

GDPR: article 5(1) (*f*)

- data subjects have eight fundamental rights (which are not absolute) under the GDPR, namely:

1. the right to access personal data and the controller must respond to that request within 30 days (article 15);
2. the right to modification, including the correction or errors and the updating of incomplete information (article 16);
3. the right to erasure – also referred to as the right to deletion or the right to be forgotten – allows a data subject to stop all processing of their data and request their personal data be deleted (article 17);
4. the right to restrict or stop data processing (article 18);
5. the right to be informed or notified about the uses of (and rectification or erasure of) their personal data in a clear manner and be told the actions that can be taken if they feel their rights are being impeded (article 19);
6. the right to data portability in terms of which a data subject can request that their personal data file be sent electronically to a third party in a commonly used, machine readable format, if doing so is technically feasible (article 20);
7. the right to object to data processing and if the request is rejected by a controller, the data subject has the right to object (article 21); and
8. the right to refuse the automated processing of their personal data to make decisions about them if that significantly affects the data subject or produces legal effects, such as automated profiling (article 22) (These rights do not form part of the seven data protection principles set out in article 5).

ENSpired (compliance) tip of the week

- the Promotion of Access to information Act, 2000 manual is a good place to address data subject access requests and the right to be forgotten. In addition, organisations should have data sharing and data subject access request policies.

case spotlight

Delete that number; he doesn't want to hear from you!

- in August 2019, the Data State Inspectorate of Latvia imposed a fine of EUR7 000 on a merchant who has an online store for infringing the "right to be forgotten" pursuant to article 17 of the GDPR. He was repeatedly requested by a data subject to delete all his personal data, in particular, his mobile phone number, which the merchant had received as part of an order. The merchant failed to delete the number and repeatedly sent advertising messages by SMS to that number.

cybersecurity

Penetration testing: how can it help you?

- regular penetration testing is an avenue companies can use to test the resilience of their cybersecurity measures.
- penetration testing, also referred to as pen testing (or pen tests), is an intentional simulated real world attack on a network, application, or system that identifies

vulnerabilities and weaknesses. Penetration tests are part of an industry recognised approach to identifying and quantifying risk.

- they actively attempt to "exploit" vulnerabilities and exposures in a company's infrastructure, applications, people and processes. Through exploitation, penetration tests are able to provide context around the vulnerability, impact, threat and the likelihood of a breach in an information asset.
- the benefits of regular penetration testing include:
    - **managing risk timeously and effectively:** it identifies vulnerabilities in your environment and allows you to remediate them, before an adversary takes advantage of them.
    - **protecting clients, partners and third parties:** it shows clients (or gives them comfort) that you take cybersecurity seriously, and it builds trust and a good reputation, that you're doing everything you can to mitigate the risks of a cyber breach.
    - **allows you to understand the environment:** a penetration test allows you to understand what is going on in the environment around you, and it helps you to understand the types of cyber-attacks that your organisation may face.
    - **identifies weaknesses you didnt know were there:** penetration testing looks for the potential backdoors into your network that exist without your knowledge.
- ENSafrica's TMT team has vast experience working with recognised and reputable service providers in this particular area of cybersecurity. We also strive to ensure that we couple our legal solutions with sound technical partner solutions, including using best of breed technology as well as change management expertise.

what? why?

Legitimate interest opinions?

- as discussed in a previous issue of Privacy in Brief, POPIA provides that, in the absence of consent, a responsible party may be able to process personal information if there is another ground of justification.
- two of these grounds refer to legitimate interest, namely where the processing protects a legitimate interest of the data subject or where the processing is necessary for pursuing the legitimate interests of the responsible party/third party to whom information is supplied.
- legitimate interest is an undefined term in POPIA but can be seen as the most flexible ground of justification. It's likely to be most appropriately used where processing is done as would be reasonably expected by data subjects or where the processing has a minimal privacy impact. However, this means taking on extra responsibility for considering and protecting data subjects' rights and interests.
- the best way to demonstrate a responsible party's compliance is to keep a record of the legitimate interest assessment or legitimate interest opinion undertaken. A legitimate interest assessment or legitimate interest opinion is one that identifies a legitimate interest, shows why the processing is necessary to achieve it, and balances the requirement for processing against the data subject's interests, rights and freedoms. The interest could be a commercial, individual or broader social interest. An important consideration is that the processing must be necessary.

If the same result can be achieved in another way, then it is likely that the legitimate interest will not apply.

data commercialisation

The law is not enough

- a common thread across the world is that data privacy laws and legal processes are simply not agile enough to keep up with technological developments. In fact, even sections of POPIA (which is due to commence on 1 April 2020) are in a sense already outdated because technology has leapfrogged the law.
- for an organisation to truly give meaning and effect to protecting privacy and compliance with privacy laws, legal compliance needs to be coupled with technological solutions which are adaptive, responsive and updated in line with new developments in technology as well as new threats.
- from a commercial perspective, this presents an enormous opportunity for technology companies and resellers to piggy-back off the law by securing rights to innovative, responsive and globally successful technologies in data protection, cybersecurity, data retention and data commercialisation. In this instance, the commercial benefit lies not only in being able to assist clients with monetising data, but also securing data in a manner that is compliant with global best practice, the requirements of legislation and regulation as well as industry acceptable standards.
- as a technology company or reseller or would-be reseller of relatable products and services, building new streams of revenue off the back of legislation such as POPIA starts with proper contracting in order to secure rights to latest technology and innovation.
- speak to our team of technology and privacy law experts who can assist in protecting your company's interests in acquiring or granting rights in products and/or services, and who are commercially minded enough to assist in building your revenue models to maximise the opportunities presented by legislation such as POPIA.

ENSide Africa

Ghana

- Ghana has enacted the Data Protection Act, 2012 (the "**Act**") to regulate and protect the privacy and personal information of data subjects.
- the Act establishes a Data Protection Commission (the "**Commission**"), which is mandated to ensure compliance with the Act.
- the Act also requires that data controllers and data processors register with the Commission. There are eight principles for processing personal information which include:
    1. accountability;
    2. lawfulness of processing;
    3. specification of purpose;
    4. compatibility of further processing with purpose of collection;
    5. quality of information;
    6. openness;

7. data security safeguards; and
8. data subject participation.

- non-compliance with provisions of the Act may attract a fine or criminal sanctions depending on the nature of non-compliance.

strange times

Never mind your nosy aunt, AI is your new matchmaker

- long gone are the days where you need to rely on a family member (usually an older nosy one at that) to set you up on awkward dates.
- technology is now capable of assisting many lonely souls with their romantic endeavours, whether this be marriage, something less permanent, or even a platonic pen pal.
- these dating applications are now increasingly using artificial intelligence ("**AI**") tools to assist in the matchmaking process. AI combined with the various dating applications is helping thousands of people all over the world find their perfect partner in a shorter amount of time.
- the AI technology considers the data provided, in the form of user-indicated preferences and interactions on the relevant application to offer the most relevant matches – saving the love-seeking individual the hassle of having to send individual messages and scour through endless profiles.
- it has even been predicted that Tinder will in future use AI to entirely eliminate the necessity for swiping left or right by rather automatically offering up a match.
- one matchmaking service in Japan recently made headlines after it held a *konkatsu* (spouse hunting) event. The participants at the *konkatsu* wore wristbands and when they shook hands with others at the party, their profiles would appear on a tablet. These profiles would provide useful information, such as whether a person is a smoker or has previously been married, and even went so far as to facilitate conversation-making.
- some have suggested that the AI-enabled dating applications may even assist with eliminating fake profiles.
- with Valentine's Day coming up this week, we certainly wouldn't blame anyone for trying out these time-saving techniques. However, users should bear in mind that any AI technology, especially such as these we have described, is data driven.
- in order to work, the users have to divulge their preferences and often very personal or intimate details about themselves. For example, the Japanese matchmaking service discussed above requires a user to answer over 100 questions on registration.
- the AI technology then also utilises your previous interactions with others and the applications to gather further information about your romantic preferences and therefore, you.
- Kaspersky has revealed that, even without deploying AI technology, many of the top dating sites and apps are not sufficiently secure. Perhaps this is something to bear in mind before jumping on this bandwagon, maybe a nosy family member may just be more tolerable!

in the news

- **EU:** the European Union is considering a ban on the use of facial recognition in public areas for three to five years in order to come up with rules and regulations in order to prevent abuse of the technology.
- **Facebook:** a judge in the state of Massachusetts has ordered Facebook to hand over data of thousands of apps that Facebook suspected may have caused privacy violations.
- **UK:** the Information Commissioner's Office has published a new code of conduct to protect children's privacy online, it hopes that the code will come into effect in 2021 and includes a set of 15 standards that online services should meet to protect children's privacy.

upcoming events

the next edition of Privacy in Brief will have details of our upcoming monthly POPIA and related seminars. For bespoke training for your organisation, please contact one of our privacy experts.

our services

ENSafrica has a highly specialised team of privacy and cybersecurity lawyers with deep expertise and experience in assisting clients with all aspects of POPIA compliance, GDPR assistance, cybersecurity and insurance, and data commercialisation. Our unique services includes the provision of a POPIA Toolkit, which contains data protection policies and other documentation which can be tailor-made for your organisation and help fast track your organisation's POPIA compliance journey. We also provide training on awareness initiatives, risk assessments, privacy impact assessments, policy and procedure implementation, and also provide a helpful service to Information Officers requiring support in implementing POPIA.

Contacts

Ridwaan Boda
Executive | Technology, Media and Telecommunications
+27 83 345 1119
rboda@ENSafrica.com

Era Gunning
Executive | Banking and Finance
+27 82 788 0827
egunning@ENSafrica.com

Wilmari Strachan
Executive | Technology, Media and Telecommunications
+27 82 926 8751
wstrachan@ENSafrica.com

Rakhee Dullabh
Senior Associate | Technology, Media and Telecommunications
+27 82 509 6565
rdullabh@ENSafrica.com