ENSafrica | Africa's largest law firm **issue 9** | 2020-02

ENSafrica privacy in brief

issue 9 | ENSafrica's newsworthy stories on data privacy and compliance.

feature topic

POPIA is coming. What should we do?

- subject to the South African President, the Protection of Personal Information Act, 2013 ("**POPIA**") is due to come into effect on 1 April 2020. What should organisations do to start getting ready for POPIA?
    1. **don't panic** – POPIA has an implementation period of 12 months from 1 April 2020, so it is not too late to start your compliance journey.
    2. **don't procrastinate** – POPIA compliance is not an overnight event, it is a journey. While number one above applies, this does not mean that organisations should wait until 2021 to start their compliance journeys. Start as early as possible.
    3. **seize the opportunity** – a well-structured POPIA compliance journey can actually lead to profit for organisations who use the journey to get smart about how data is used.
    4. **obtain executive buy-in** – without backing of management and allocation of resources, POPIA compliance will not be achieved. The fact that the CEO of a private organisation is the default Information Officer and POPIA as read with the Promotion of Access to Information Act, 2000 ("**PAIA**") imposes personal liability on the Information Officer in certain instances should be incentive enough to comply. The threat of fines, penalties and worst of all, reputational loss, should be even bigger incentives to comply.
    5. **find trusted and experienced advisors** – if we learn from examples of what happened in Europe prior to the General Data Protection Regulation ("**GDPR**") implementation date as well as the popping up of market entrants holding themselves out to the "POPIA experts", pick your POPIA advisor carefully. Vet and verify their experience and claim to expertise and ensure that they are not just being opportunistic in offering services after attending one seminar on POPIA.
    6. **it's not just law** – organisations will need a mix of legal, technological and change management solutions to get compliant. ENSafrica (together with select reputable IT companies) offers an end-to-end compliance solution which factors in legal tools (such as our POPIA Toolkit), use of technology, and change management professionals where needed.
    7. **use quick wins** – the POPIA Toolkit designed by ENSafrica helps organisations to fast track their compliance efforts.

8. **call or email our POPIA experts, it's virtually free** – the call may cost you just a few minutes in airtime spend (the email a little in data), but we promise we will not charge you for our time taken on the call.

POPIA in brief

Direct marketing in terms of POPIA and GDPR

- there is a widespread misconception in the market at the moment about what consent to electronic direct marketing (ie, opt in clauses) means. This is partly because it is often assumed that the European Union ("**EU**") sets the "gold standard" for data protection and that any opt-in consent clauses that meet the EU requirements should suffice in South Africa, too. But this is not correct.
- firstly, it is important to distinguish between the situation in the EU and that in South Africa.
    - sending of direct marketing communications in the EU is regulated by both the GDPR and the ePrivacy Directive ("**ePD**") (which will soon be replaced by the ePrivacy Regulation ("**ePR**")).
    - as a general rule, article 16(1) of the ePR requires companies to obtain end-users' consent before sending electronic direct marketing communications to them (ie, an "opt-in" requirement). This consent is defined by reference to articles 4(11) and 7 of the GDPR and must be a freely given, specific, informed and unambiguous indication of wishes expressed by a statement of a clear affirmative action. Often, such consent is expressed by ticking a box.
    - while opt-in remains the standard for direct marketing communications in electronic form in the EU, article 16(2) of the ePR provides an exemption to that rule, known as the "soft opt-in", where three conditions need to be met:
        - the electronic contact details must have been obtained by the person wishing to send direct marketing (ie, the controller) from end-users who are natural persons, in the context of the sale or purchase of a product or a service;
        - the end-users must clearly and distinctly be given the opportunity to object, free of charge and in an easy manner, to the use of their contact details for direct marketing at the time of collection of these contact details. If that end-user has not initially refused that use, they must also be able to opt out each time the controller sends a message to that end-user for the purpose of direct marketing; and
        - the electronic contact details may only be used for direct marketing of the controller's own similar products or services.
- in South Africa, once POPIA comes into force, while the "soft opt-in" will be almost identical to ePR in section 69(3) of POPIA, the "opt-in" requirements will be a lot more stringently regulated under section 69(2).
- section 69(3) provides that a responsible party may only process the personal information of a data subject who is a customer of the responsible party for the purpose of direct marketing of the responsible party's own similar products or services if:

    - the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
    - the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details at the time when the information was collected and on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.
- section 69(2) provides that a responsible party may approach a data subject whose consent is required for direct marketing by electronic means, and who has not previously withheld his or her consent, only once in the prescribed manner and form in order to request the consent of that data subject.
- the prescribed manner and form were promulgated in terms of regulation 6 of the POPIA Regulations, which stipulates that a responsible party must submit a request for written consent to that data subject on the prescribed Form 4.
- special attention should be given to the following definitions set out in the POPIA Regulations when interpreting the requirements of Regulation 6:
    - "submit" means submit by data message, electronic communication; registered post; electronic mail; facsimile; and personal delivery;
    - “data message” includes a data message as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (“**ECTA**”) (ie, data generated, sent, received or stored by electronic means and includes voice, where the voice is used in an automated transaction; and a stored record);
    - “writing” includes writing as referred to in section 12 of ECTA (ie, a legal requirement that a document or information must be in writing will be met if it is in the form of a data message; and accessible in a manner usable for subsequent reference);
    - “signature” includes an electronic signature as defined in section 1 of ECTA (ie, data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature); and
    - “form(s)” means a form referred to in the annexures to the POPIA Regulations or any form which is substantially similar. The meaning of “substantially similar” within the context of the POPIA Regulations has, of course, not yet been judicially considered. The court has, however, in different circumstances, held that the word "substantially" means “in the main” or “in its principal essentials” and that a thing is “similar” to another if without being identical with it, there is a resemblance in some relevant respect. In our view, the phrase "substantially similar", in the context of the POPIA Regulations, means that any consent clause, for purposes of direct marketing by electronic means, must resemble or contain the principal essentials of Form 4, but does not have to be identical to it.
- as such, consent can be obtained in a form containing the essential elements of Form 4, sent to the data subject by means of a data message, such as an email or USSD link, and signed by the data subject by means of an electronic signature. This will make getting Form 4 consent considerably simpler.

ENSpired (compliance) tip of the week

- "direct marketing", in terms of POPIA, means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
    - promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
    - requesting the data subject to make a donation of any kind for any reason.
- the sending of newsletters and the like would probably constitute direct marketing. In addition, certain forms of targeted social media marketing would also fall to be regulated as direct marketing under POPIA.
- all responsible parties who send direct marketing by electronic means (including by means of SMS and email) should put the necessary prescribed consents in place for non-customers and ensure that customers are informed of the fact that they may be sent electronic direct marketing. In our experience, the use of well-drafted privacy policies work particularly well in these circumstances.

case spotlight

- a mobile network operator received a fine from the Information Commissioner's Office ("**ICO**") of EUR100 000 for sending more than 2.5-million direct marketing text messages to customers without their consent.
- the mobile network service provider raised the defence that the texts were "service messages" and not direct marketing messages. However, the ICO disagreed and stated that the messages promoted the company's products and services. If a service message contains promotional content, then direct marketing rules apply and consent is required.
- furthermore, under direct marketing rules, customers should always be given a simple way to opt out of marketing when their details are first collected and in every message sent.

cybersecurity

Trojan keyloggers: What are they and how to detect if you have been keylogged?

- a keylogger (or Trojan keylogger) is a program that logs keyboard keystrokes. Essentially, the main risk of having a keylogger virus on your computer is that it can very easily keep track of every single keystroke you enter through your keyboard, and this includes every credential. They are attached to a regular, sometimes functioning program so that it doesn't seem like anything nefarious is installed on your computer.
- once the virus keylogger is installed, the virus keeps track of all the keys and the logs are sent over the internet back to the hacker offsite. If you have a keylogger virus

and you are using your keyboard to enter information anywhere, you can be certain that the virus is well aware of your details. This is true whether it's in an offline program like Microsoft Word or an online website like your bank or social media account.

- in some instances, depending on its nature, keystroke malware can refrain from recording the keystrokes until a certain activity is registered. For example, the program might wait until you open your web browser and access a specific bank website before it starts.
- the easiest way for a Trojan keylogger to reach your computer is when your antivirus software is outdated or turned off. Virus protection tools that are not updated cannot fend against new keylogger programs.
- keyloggers are downloaded through an executable file of some sort, like an .exe file. That's how any program on your computer is able to launch. However, since most programs are in the .exe format, it's next to impossible to avoid all .exe files in an attempt to avoid keyloggers. One thing you can watch out for, is from where you're downloading your software. Most well-known websites will scan all their programs before releasing them to the public, in which case you can be certain that they don't contain malware, but that isn't true for every website on the internet.
- as long as you have an updated antivirus program running, you should be secure enough to thwart any keylogging attempt. Some other tools don't necessarily remove keylogger viruses but instead, avoid using the keyboard so that the keylogger doesn't understand what is being typed. For example, the LastPass password manager can insert your passwords into a web form through a few mouse clicks, and a virtual keyboard lets you type using your mouse.

what? why?

- data touch points are not something to get touchy about but they are definitely something worth considering!
- understanding the data “touch points” in your environment is a critical step in your data privacy compliance journey. A “touch point” is the intersection of where data, and in this context, personal information, is processed in an organisation or processed outside of the organisation by a third party.
- this can be the collection of personal information of customers as they enter your premises, the destruction of personal information as you dispose of your waste, the use of customer information to send direct marketing communications, the transfer of specific employee information for reporting purposes or even the use of technologies external to the organisation such as cloud computing.
- identifying all of the touch points in your organisation will give you a clear map of what, how and by who personal information is currently being processed. As part of this initiative, the following should be considered:
    - why and for what purpose is the personal information being processed?
    - how sensitive is the personal information? Does it include special personal information or personal information of children?
    - how aware is the data subject of the processing of their personal information?

    - is the personal information being stored? Is such storage secure?
    - for how long is the personal information kept? How is it destroyed when no longer needed?
    - is the personal information being transferred (whether internally or externally)? Why and to whom?
- knowing where your touch points are and what personal information is being processed will inform your data privacy strategy, including how to responsibly and effectively mitigate against risk of unlawful processing, and will also improve your business through data insights and your customers' experience. It is the foundation of any sound data commercialisation strategy.

data commercialisation

- this week, we remind the reader of the commercial benefits of a well-structured POPIA compliance programme:
    - use the POPIA compliance journey to protect your organisation from the threat of fines, penalties, claims and reputational loss;
    - use the data insights derived from the journey to adopt a formal data commercialisation plan. According to research company Forrestor, "Many companies have derived value from that data, either through cost savings from operational insights or revenue growth from customer insights";
    - in addition, companies may seek to:
        - use data to create new products or services to enhance the customer relationship
        - create internal efficiencies by applying data insights
        - generate additional revenue streams by "selling" data (in a lawful manner
    - a well-structured POPIA compliance will lead to improved cybersecurity and protection against cyber risks;
    - a well-defined training programme will help protect staff (and their families) in both their professional and personal lives from data threats;
    - use and/or commercial exploitation of new and emerging technologies such as AI, IoT, drones and the like are mitigated;
    - protect your data assets and remember the (much abused) adage, "data is the new oil".
- for training and assistance in developing your organisations data commercialisation strategy, contact our expert team who will guide you through the journey.

ENSide Africa

Botswana

- Botswana passed the Data Protection Act in 2018, however it is still awaiting commencement.

- the Act establishes an Information and Data Protection Commission, which will be responsible for ensuring compliance with the Act.
- the Act applies to processing of personal data entered into a file or for controllers situated in Botswana, or where the controller is not in Botswana, personal data is processed using means situated in Botswana.
- the Act prescribes fines and imprisonment for penalties for violations of its provisions. Although the Act has not yet commenced, there is a transition period of 12 months from commencement within which all processing of personal data must be made compliant with the Act.

strange times

A rose by any other name…

- government surveillance and white hat hackers seem like unlikely bed fellows, but they most certainly are. Japan has donned its white hat in an effort to ramp up cybersecurity leading up to the 2020 Tokyo Olympics.
- that said, these efforts appear to extend beyond the Olympics, as the programme may last up to five years (white hat government surveillance?). We pause here for a moment to recall the revelation that Japan's minister in charge of cybersecurity has admitted that he has never used a computer in his professional life and appeared confused by the concept of a USB drive when asked further questions. Nonetheless, he surprised us all by coming up with a novel and extreme form of penetration testing. But let's be fair – he delegated any computering to his underlings.
- the programme, which was approved early last year, authorised Japan's National Institute of Information and Communications Technology ("**NICT**") to try to hack into internet-connected devices ("**IoT devices**") in homes and offices around Japan. The programme kicked into action in March 2019 with the NICT using default passwords and password dictionaries to try to break into about 200-million devices, starting with webcams (kudos to all those who have made the effort to cover their webcam) and routers.
- the plan is that when the NICT successfully gains access to a device, the owner will be contacted and advised to improve security measures. Some have asked the obvious question – why not simply advise everybody to improve security measures before going to the extreme of hacking them? But of course, let's give credit where it is due, we have written about the vast amount of personal information and vulnerabilities apparent when it comes to IoT devices and the NICT itself has also determined in a separate study in 2017 that IoT devices were targeted in 54% of cyberattacks.
- security is certainly a concern when it comes to IoT, but we can't always blame a weak password for that. Humans tend to be the weakness and many experts have expressed concern that the NICT will be, as a by-product of its efforts, creating a list of vulnerable IoT devices for hatless hackers to exploit. Furthermore, it is unclear how the Japanese Government will further use the wealth of data likely to be collected in its efforts.

- the real question is however, should the developers of the IoT devices themselves be put under more pressure to develop secure systems, or should we wait for our government to don their white hat?

in the news

- **Facebook**: The social media platform had planned to launch its dating service in Europe but it had been called off because it failed to give the EU data regulator adequate notice including failing to demonstrate it had performed a legally required assessment of privacy risks.
- **Estée Lauder**: An unprotected database containing 440-million records owned by Estée Lauder has been exposed online. The database contained plain text email addresses belonging to users of a company-owned education platform.
- **EU**: Last year, the EU proposed a ban on the use of facial recognition technology for a period of five years so that it can study the impact of its use. However, this year the European Commission will encourage member states to develop their own rules, regarding the use of the technology.

upcoming events

- click here for 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