Deloitte.
Legal

Africa | Risk Advisory | January 2018

# Deloitte Legal – Representing Tomorrow
International Data Privacy Day: 28 January 2018

After International Data Privacy Day 2018, we revisit some of the headlining data privacy stories of 2017, both locally and internationally, in the world of privacy and data protection.

## South Africa: Information Regulator – further developments

Another year has passed and we move ever closer to the effective date of the Protection of Personal Information Act 4 of 2013 ("POPIA") being proclaimed by Presidential proclamation in the Government Gazette ("Gazette"). Advocate Pansy Tlakula ("Tlakula"), the appointed chairperson of South Africa's Information Regulator ("Regulator"), indicated in early 2017 that the Regulator is currently ensuring that its required personnel, financial and infrastructural requirements are in order, so that the effective date of POPIA may become a reality, thus triggering the 12-month grace period for compliance by both public and private organisations who process personal information.

The draft Regulations were, in terms of section 112 of POPIA, published by the Regulator on 8 September 2017 in the Gazette. Interested parties were given until 7 November 2017 to submit comments thereon, if any, and the Regulator visited all 9 provinces in South Africa with the aim of engaging the public and soliciting comments on the draft Regulations. The draft Regulations which were published, relate, inter alia, to the following aspects:

- the manner in which a data subject (a natural/juristic person whose data is collected/processed) may, in terms of section 11(3)(a) of POPIA, object to the processing of their personal information by a responsible party (the organisation which processes the personal data), including the requisite form to be completed by the data subject for this purpose;

- the manner in which a data subject must, in terms of section 24(1) of POPIA, request a responsible party to correct/delete or destroy/delete any records containing the personal data of that data subject, including the requisite form to be completed by the data subject for this purpose;

- the duties and responsibilities of information officers in terms of section 55 of POPIA, which include, inter alia, that the information officers should develop, implement and monitor a compliance framework within their organisations for purposes of complying with POPIA;

- how responsible parties should, in compliance with section 69(2) of POPIA, go about requesting consent from data subjects in order to process their personal data for the purposes of direct marketing by means of unsolicited electronic communications (such as email, for example), including the requisite form to be completed by responsible parties and provided to data subjects for this purpose; and

- how complaints/grievances contemplated in section 74(1) and (2) are to be submitted to the Regulator, including the requisite forms to be completed by the aggrieved person/s for this purpose.

We now await the Regulator's consideration of all comments that were received from interested parties and thereafter the tabling of the amended draft Regulations in Parliament for finalisation and voting.

## South Africa's Largest Ever Data Breach

In October 2017, it was discovered by a prominent Australian security developer and information security expert, Troy Hunt ("Hunt"), that an enormous trove of data (approximately 27 gigabytes) was uploaded onto a website which was hosted in the cloud. This carried substantial risks of data leakage as the data was allegedly hosted on an unsecured server. The data in question included, inter alia, elements such as name, surname, government-issued identity number, physical home address, employment history and income of approximately 33 million South African citizens (including children and deceased persons). According to certain media sources, even the personal data of prominent politicians such as Malusi Gigaba and President Jacob Zuma were contained in the trove of leaked personal data files. There is no certainty as to how long the data files have been available on the web server for. As such, they were accessible by anyone and it is not certain how many South African citizens' identities may have been used unlawfully.

Hunt was able to discover the leaked data files by tracing them through the internet protocol address of the server in question, it was discovered that the server belongs to a real estate, corporate investment and skills development company called Jigsaw Holdings Proprietary Limited ("Jigsaw Holdings"), which is the holding company of well-known real estate entities such as Aida and Realty 1.

It is clear that the breach did not emanate from a hack of the website, but rather, the data was too easily accessible by almost anyone with a basic degree of technical knowledge. Further investigation by data security experts have revealed that the security on the website was significantly inadequate.

Despite the effective date of POPIA not having been proclaimed, the Regulator has indicated that this breach has brought South Africa as a country into disrepute from a data protection perspective, as international entities may be reluctant to trust entities in South Africa with their personal data. The Regulator is in the process of investigating this breach and has called upon Jigsaw Holdings to account for the breach.

South African organisations should ensure that they have adequate data breach management processes and procedures in place and should take a pro-active, risk-based approach to ensure that such breaches are prevented, alternatively adequately managed should they occur. With adequate privacy and security safeguards in place, Jigsaw Holdings could have prevented a breach of this magnitude, let alone the breach itself, from occurring.


## Pace yourself – the incriminating pacemaker

With the proliferation of technological advancement and Internet-Of-Things ("IOT") as well as Artificial Intelligence, we live in an age where technological devices know us better than we know ourselves, particularly in the course of processing and storing our personal information. Moreover, they may serve as witnesses against us. This was demonstrated in a case of arson in the state of Ohio, United States. In this instance, the man's cardiac pacing device – his "pacemaker" – incriminated him in an instance where, in the absence of the electronic data evidence derived from his pacemaker, he may potentially have evaded conviction.

Ordinarily, a pacemaker captures the personal information of the user or patient, such as heart rate and cardiac rhythms, which can reveal a substantial amount of information about the duration and intensity of any activity that the person is or may have been involved in at any particular point in time. This is precisely what occurred here – the personal information in question captured and stored by the pacemaker proved to be the individual's downfall.

September 2017, Ross Compton ("Mr Compton"), aged 59, from Ohio State, was convicted on charges of aggravated arson and insurance fraud due to allegations of starting a fire at his Ohio home. In his initial statement to the investigative authorities and police, he indicated that upon becoming aware of the fire, he was able to pack a suitcase and some bags with his belongings, break his bedroom window with a cane, carrying his belongings with him and flee from the fire. The police were of the view that Mr Compton's initial statement did not correlate with evidence discovered at the fire. However, the evidence was at the time circumstantial at most, and further evidence would be required to provide weight in order to secure a conviction against Mr Compton. The police secured a warrant for the electronic data stored on Mr Compton's pacemaker which included his cardiac rhythms, heart rate and pacer demand before, during and after the fire. A cardiologist who reviewed this data indicated to police that, based on Mr Compton's heart condition, it was highly unlikely that he would have been able to pack his bags, break his bedroom window, pick up and throw his bags out of the window and then rush to his car thereafter – all within a short space of time.

It's clear that the digital ramifications of IOT technology are quite far-reaching. Mr Compton's own heart (and life-saving) device processed and stored personal information, the absence of which, would potentially have meant that he would be a free man today. On the other hand, IOT technology, despite having far-reaching data privacy consequences, could help deter crime.

## General Data Protection Regulation ("GDPR"): the wait is over

The effective date of 25 May 2018 for enforcement of the GDPR is fast approaching and organisations which process personal information of European Union ("EU") residents should by now, at the very least, have a compliance implementation plan and roadmap in place.

So, what are the implications of the GDPR becoming fully enforceable on 25 May 2018? Data privacy laws such as the GDPR have been introduced to ensure that organisations conduct their undertakings in a manner that respects and upholds individuals' right to privacy and data protection. Accordingly, complying with the GDPR is a business imperative, not a compliance tick-box exercise or 'grudge purchase', and would enhance any organisation's ability to engage with EU customers, business partners and other stakeholders in order to maximise its business objectives. The competitive advantages of complying with the GDPR cannot be overstated. As far as organisations having commercial dealings with EU data subjects is concerned, EU stakeholders would in all likelihood be more comfortable to engage with organisations whose business processes and procedures demonstrate their accountability, in alignment with GDPR requirements.

Organisations which target or do business with EU data subjects need to be aware that the data protection principles delineated in their local data privacy laws, if any, may potentially be similar to (or be primarily based on) the GDPR principles, as GDPR privacy principles are some of the most progressive globally. Accordingly, by organisations ensuring that regulatory, organisational and technical measures are in place for compliance with their local data privacy laws may potentially enable GDPR compliance to a certain extent. It is thus, a 'rationalisation' exercise, which should be applied to map the similarities and differences between an organisation's local data privacy laws (if any) and the GDPR, and mapping out compliance goals accordingly. This may enable organisations to ensure that there is an integration of their existing data privacy compliance programmes (if any) into any envisaged GDPR compliance initiatives.

A risk-based approach should be applied to determine which specific risks the organisation faces – in light of its industry, geographic footprint, types and volume of personal data it processes in order to further business objectives. The organisation's data privacy control environment should be commensurate with these factors. It is crucial to note that the GDPR may carry a higher standard of compliance; hence an organisation's processes and procedures should be nuanced, where necessary.

There is no one-size-fits-all solution to data privacy GDPR compliance. Due to the imminence of the GDPR, full compliance by the enforcement date will be challenging, as achieving full data privacy compliance is a complex and lengthy process which, depending on the size and industry of the organisation in question, could take between two and five years to effectively embed into the organisation's business operations. It involves a significant overhaul of an organisation's governance structures, people, processes and technology. Nonetheless, to prevent last-minute panic and avoid a "wait and see" approach, organisations should implement certain cost-effective "quick wins" to get the ball rolling and ensure that they are on the path to GDPR compliance. These quick wins should ideally be initiated within an organisation's high-risk areas which process personal information, and they would help to demonstrate to any EU data protection authority, that your organisation is able to demonstrate GDPR compliance to a reasonable degree.

## For more information, contact:


**Dean Chivers**
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Tel: +27 11 806 5159
Email: dechivers@deloitte.co.za

**Daniella Kafouris**
Associate Director: Risk Advisory Southern Africa
Tel: +27 11 209 8101
Email: dkafouris@deloitte.co.za