Data-breaches: some valuable lessons learned and handy tips

With the proclamation of the commencement date of the Protection of Personal Information, 2013 (“POPIA”) expected imminently, the extensive data breach notification obligations imposed on organisations in terms of POPIA are of significant importance. On the occurrence of a data breach, organisations are required to notify the Information Regulator and the data subject(s) whose information has been breached, at a bare minimum, of the following:

- the identity of the party who accessed/acquired the data (if known);
- the possible consequences/effect of the breach;
- the measures taken (or proposed to be taken) by an organisation to remedy the breach; and
- the measures the data subject (whose information has been breached) should take to mitigate any possible adverse effects of the breach.

While data breach notifications to the Information Regulator are currently voluntary (and while there will be a grace period of 12 months from the commencement of POPIA for organisations to comply), some valuable lessons can be learned from jurisdictions where data breach reporting is already mandatory.

Data breach notifications became mandatory in Canada on 1 November 2018. Marking a year on from this date, the Office of the Privacy Commissioner of Canada published some key lessons learned and gave some tips, some of which we set out below, which are useful and relevant to organisations in South Africa:

- while data breaches arose out of a variety of causes (including loss, theft and accidental disclosure), the majority of reported data breaches arose from unauthorised access to data (by “snooping” employees as well as external parties);
- organisations should take steps to fully understand what type of personal information they have, how the organisation gathers personal information, where it is stored, who has access to it and what they do with it;
• as there has been a significant increase in the number of reported data breaches, this serves as a reminder to organisations to carefully consider the safeguards they have in place to protect personal information;

• risk and vulnerability assessments should be carried out regularly by organisations in order to identify technical vulnerabilities, to check whether third parties who collect personal information on their behalf have sufficient protections in place, as well as to ensure that employees are aware of their privacy obligations and risks; and

• be aware of breaches in your industry – as similar methods are usually used by hackers, being aware of other incidents could prevent your business from being a victim.

Having a comprehensive cyber insurance policy in place can greatly assist an organisation that suffers a data breach – cyber insurance coverage typically covers the costs incurred during the notification process, which process should ideally include the advices and assistance of a legal representative in preparing the notification to the Information Regulator, in order to ensure compliance with the statutory notification obligation.

**POPIA in brief**

**Condition 7: security measures**

The 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 loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information. The organisation must have due regard to generally accepted information practices and procedures which may apply to it generally or may be required in terms of specific industry or professional rules and regulations.

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 the Regulator; and the data subject, unless the identity of such data subject cannot be established or if a public body responsible for the prevention or the detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification referred to above must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system.

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

Personal data must be processed in a manner that ensures appropriate security of the data,
including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (the ‘integrity and confidentiality’ principle).

**ENSpired (compliance) tip of the week**

Data security is an IT and an operational issue. The implementation of organisational measures, such as clean-desk and printer policies, are as important as IT security.

In addition, organisations should be prepared for cyber breaches. In order to guard against the potential loss of a cyber-breach, cyber insurance can be taken out by an organisation. It is important that an organisation considers the provisions of its cyber insurance policy when planning or drafting a data breach policy. An insurer might prescribe certain steps to be take when an incident occurs and failure to comply might result in an insurer repudiating a claim.

**case spotlight**

In March 2019, the Norwegian Supervisory Authority imposed a fine of EUR170 000 on a municipality for not having implemented sufficient technical and organisational measures to ensure information security. The incident relates to the unauthorised access to computer files with usernames and passwords of over 35 000 user accounts in the municipality’s computer system, including information of employees and pupils in the municipality’s primary schools.

Due to insufficient security measures, these files had not been protected and were openly accessible. Anyone could log in to the school’s various information systems, and access various categories of personal data relating to the pupils and employees of the schools. The fact that the breach compromised personal data of over 35 000 individuals, coupled with the fact that the majority of these were children, were found to be aggravating factors. The municipality had also been warned on a number of occasion by the authority and an internal whistle-blower, that the data security was inadequate.

**cybersecurity**

One of the world’s first most notable cyber-attacks happened in the 1980’s. Robert Morris wanted to know how big the internet was, so he wrote a program that would travel from computer to computer and ask each computer to send a signal back to a control server, which would then keep count of the number of pings.

The program worked so well that large sections of the internet became clogged up. This program became the first of a particular type of cyber-attack called “Distributed Denial of Service (“DDOS”). A DDOS attack is an attempt to disrupt normal traffic of a targeted server,
service or network by overwhelming the target or its surrounding infrastructure with a flood of traffic.

Since then cyber-attacks have evolved and have become more sinister. Criminals have found a way of profiting by exploiting the vulnerabilities of computer systems. Participation in society today demands some level of connectivity and technology bestows valuable benefits, but it also allows for criminal activity. Given the significant increase in internet access and societies’ growing reliance on computer systems, new laws are required to deal with the complexity of crimes that happen in cyberspace.

South African law has been slowly developing in order to respond to the modern day threat of cybercrimes. The first piece of law which specifically addresses cyber-crime is the Electronic Communications and Transactions Act, 2002 (“ECTA”). ECTA criminalises a limited number of offences which include unauthorised access to, interception of or interference with data, computer-related extortion, fraud and forgery and attempting, and aiding and abetting any of the above mentioned offences. Because ECTA is so limited, and recognising the growing number of cyber-attacks in South Africa, specific comprehensive legislation was required to deal with complexities that cyber-attacks pose.

In 2017 the draft Cybercrimes and Cybersecurity Bill was submitted to Parliament and included a cybercrimes and cybersecurity section. The cybersecurity section raised various concerns around freedom of expression and internet censorship. As a result, the cybersecurity section was removed from its successor, the Cybercrime Bill.

The objectives of the Cybercrime Bill essentially include the codification and imposition of penalties on cybercrimes. The Cybercrime Bill now deals with offences relating to cybercrimes, jurisdiction of the courts, powers of investigation, search, seizure and access, evidence gathering, the establishment of a designated point of contact, reporting obligations and penalties.

Once the Cybercrimes Bill becomes effective, certain organisations such as electronic communications service providers and financial institutions will be required to cooperate with law enforcement in relation to the investigation of cybercrimes and will be under the obligation to report cyber offences within 72 hours of becoming aware of them.

These organisations will also be required to retain certain data relating to an investigation. It is important that organisations are aware of their obligations in order to comply with the Cybercrimes Bill and to avoid penalties.

We recommend that organisations adopt a proactive approach by introducing policies related to cybersecurity and a breach response policy as well as general cybersecurity awareness training of staff.

Data Retention Policy: What? Why?
A lot of us tend to find it difficult to get rid of things and declutter, this even holds true for organisations and the relationship that they have with their data. However, POPIA requires that organisations let go of any hoarder tendencies and only keep what is necessary. A data retention policy will help an organisation tidy up its data.

A data retention or records retention policy ensures that an organisation manages its compliance with laws that specify periods for which data or records must be held. For example, ECTA requires that a data controller keeps a record of personal information for the period that it is used and at least one year thereafter. POPIA specifies that records of personal information must only be retained for the period required to achieve the purpose for which the information was collected or processed. Unless otherwise required or authorised by law, agreed to in a contract or where consent has been obtained, personal information must be deleted, destroyed or de-identified as soon as reasonably possible after a responsible party is no longer authorised to process that information.

Based on the above, a good data retention policy considers the following:

- input and guidance from all stakeholders in the organisation, including employees responsible for data retention settings (IT), legal counsel, managers, supervisors, and anyone who deals with the management or compilation of financial reports;
- all laws, regulations, policies and codes of conduct that would apply to your organisation; and
- the defined data categories that are covered in the policy, which should as a minimum include documents, emails, customer records, transactional information, contracts, employee records, sales, invoice and billing information, tax and accounting documentation.

Like most policies, a data retention policy is only effective if all employees are aware of and understand the organisation’s policy. As a result, awareness and training with affected employees is always necessary in ensuring that the policy is adhered to. This policy is an important tool in helping an organisation avoid civil, criminal or financial penalties.
consideration to bear in mind is that notwithstanding that the target may form part of a wider group of undertakings post-transaction, this does not allow carte blanche for intergroup sharing of personal information, especially as case law from the EU suggests that each entity within a group is to be considered its own unique and individual data controller (or responsible party).

For sale of business transactions, the issues become more complex, especially as there is now a change in the responsible party. This raises a number of questions including:

- does the acquirer need to advise data subjects of the change in the responsible party?
- will fresh consent be required where consent was previously obtained to process personal information (eg consents in relation to direct marketing? If not, will a further legitimate interest opinion be required? What happens where special personal information or children’s information is being transferred as part of the sale?
- what about disparate policies between the acquirer and the target now acquired? Would an alignment of policies be required? If so, will this be post or pre-closing?
- will the information officer of the responsible party need to change?
- will PAIA manuals need to be updated?

The above issues become even more complex if the main driver of the acquisition was to acquire the target’s data (eg marketing lists, or AI data, or transaction data etc). By engaging in an M&A activity, this does not mean a carte blanche in respect of what the acquirer can do with the target’s personal information, and this becomes even more complex where special personal information or children’s information is involved. If Company A’s main purpose of the transaction is to acquire Company B’s data and personal information, it would be prudent, at a very early stage in the transaction, to consider what Company A intends to do with the personal information and data post transaction, and where relevant additional conditions precedent may need to be included in the purchase and sale agreement.

In the age where data is an asset, companies engaging in M&A activities can no longer afford to ignore the relevance of data privacy and cybersecurity in M&A transactions. The Marriot case (which we covered in part 1 of this series) is an excellent example of just how detrimental it can be to an acquirer if data privacy and cybersecurity is ignored or not considered in greater detail.
This week, we look at the data privacy regime in Nigeria. Nigeria does not have a specific Act dedicated to privacy law, however it has subsidiary legislation in place, the Nigeria Data Protection Regulation ("the Regulation"). The Regulation was issued by the National Information Technology Development Agency (NITDA) which is statutorily mandated by the NITDA Act, 2007 to develop regulations relating to, among others things, electronic governance and monitoring of the use of electronic data interchange. The Regulation applies to the processing of personal data being conducted in respect of natural persons in Nigeria and applies to persons living in Nigeria or persons of Nigerian descent outside Nigeria. The Regulation requires that a Data Protection Officer be appointed who will be responsible for driving NDPR compliance initiatives within the organization. The maximum penalty for breaches of data privacy rights can be up to NGN10-million or 2% of annual gross revenue of the preceding year, whichever is higher and based on the number of data subjects dealt with.

strange times

All I want for Christmas is ... my privacy

We have previously written about the privacy concerns associated with general household items, for example, the robotic vacuum cleaner which maps your home. We have also written about the Kayla Doll, a toy for children which was found to be susceptible to hacking and listening to your conversations. As Christmas looms we thought it best to warn you about the potentially embarrassing privacy implications which may arise should you choose to buy your special someone a toy of the adult variety. Our advice, for reasons which will be clear as you continue reading, is simply to avoid it, or at least to avoid the kinds which connect to the internet or have Bluetooth functionality (we will leave it to you to make sense of why either of those options is a possibility). We have the booming market of teledildonics – the term used for internet-connect adult pleasure products – to thank for a wealth of innovative options which are part of the internet of things.

In February this year Mozilla released a special Valentine’s Day section of its “Privacy Not Included” guide, which featured an array of gadgets from smart beds, fitness trackers and teledildonics. Of the 18 items that Mozilla assessed, only half of those were found to be secure.

There are essentially two arms of concern which arise out of the use of teledildonics. The first relates to the security of teledildonics. A lack of security could enable, not just an invasion of your most sensitive and intimate personal information, but even, possibly remote-controlled assault. This would occur where the remote control of the adult toy is taken over by a hacker and used without the recipients consent. All our research has shown that this has not happened yet and the only hacking of these toys has been conducted by security researchers. But of course, how would you know?

The second concern relates to the information that is potentially being collected by teledildonic manufacturers. Yes, this gives a whole new flavour to the typical phrase in all privacy policies – “we only collect your information to improve user experience”. In 2016, the manufacturer of the We-Vibe Rave was served with a proposed class-action lawsuit for
purportedly collecting too much information. The firm that served the papers alleged that an anonymous woman had laid the complaint saying that, had she known the company was taking real-time digital notes on how she responded to “pulse” mode compared to “cha cha” mode she may not have used the toy so eagerly along with the smartphone remote app. Even more appalling to one’s sense of dignity is the story about the Hong Kong-based manufacturer of the Lovense remote control toy. The company ended up settling a class action lawsuit after claims that the app, which required access to a mobile phone’s mic and camera for chat purposes, had a “minor bug” which meant that the mic recorded all sound clips when in use. The company explained that no audio files were stored on their servers, but for the sound feature to work it required the creation of a local cache. Either way, it’s just plain creepy.

We certainly don’t want to take the fun out of Christmas, but perhaps, if you aren’t going to read the privacy policy (that’s if the particular product even has one, some reportedly don’t), best you wrap it in one fat privacy disclaimer.

in the news

U.S: Supermarkets in the US are installing cameras that guess your age and sex in order to provide real-time targeted adverts on in-store video screens. The cameras are being criticised as being “creepy” and are raising concerns over privacy and potential discrimination.

U.K: The Divisional Court in the UK has dismissed a challenge to South Wales Police’s (“SWP”) use of Automated Facial Recognition (“AFR”). The SWP carried out a pilot scheme in which cameras are used to scan faces in large crowds in public places. Biometric data from these images is compared to a watch list of individuals known to the police and an officer will then make a decision as to whether a match exists. If no match is found, the images are deleted. Edward Bridges challenged the use of AFR by the SWP on the basis that it was unlawfully intrusive. The Court held that SWP’s use of AFR was justified as it was proportionate and struck a fair balance.

Microsoft: Microsoft has stated that it is updating the privacy provisions of its commercial cloud contracts after EU regulators found that its contracts with EU organisations failed to afford adequate protections in line with EU law.

upcoming events

Please keep a lookout for upcoming events for 2020. Happy new year and safe travels!

our services
ENSafrica has a highly specialized 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

Nicole Gabryk
Executive | Dispute Resolution
+27 82 787 9792
ngabryk@ENSafrica.com

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

This email contains confidential information. It may also be legally privileged. Interception of this email is prohibited. The information contained in this email is only for the use of the intended recipient. If you are not the intended recipient, any disclosure, copying and/or distribution of the content of this email, or the taking of any action in reliance thereon, or pursuant thereto, is strictly prohibited. Should you have received this email in error, please notify us immediately by return email. ENSafrica (ENS and its affiliates) shall not be liable if any variation is effected to any document or correspondence emailed unless that variation has been approved in writing by the attorney dealing with the matter.