KPMG

Oops… there's been another data breach

September 2020

Two weeks ago a headline ran in the media that "Data from South Africa's massive information breach is on the internet". *It related to the data breach that happened at the credit bureau, Experian, which apparently leaked the personal information of millions of South Africans and the bank accounts details of business to an alleged fraudster.*

Cyber criminals seem to be having a field day during the COVID crisis, as Life Healthcare and two insurance companies joined Experian as victims of cyber attacks. Following these attacks and the months that have followed since these attacks actually took place, questions have been raised as to whether these companies have done enough to prevent these breaches and when they have happened, to timeously detect and mitigate the risks to the individuals affected by the breaches.

Too often fraudulent activities occur as a result of avoidable data breaches, where unauthorised third parties obtain access to the personal information held by an organisation. Data breaches can be devastating to organisations and their customers, especially when the data breach results in unauthorised access to sensitive personal information of individuals which is then used for fraudulent purposes as described above.

In terms of the Protection of Personal Information Act 4 of 2013 ("POPIA") all organisations are required to secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent the unlawful access to or processing of personal information.

There is no "one-size-fits-all" approach regarding the appropriate organisational and security measures that should be taken by an organisation however organisations should be considering how they secure both physical records as well as electronic records. Some steps that an organisation could take include, for example:

- performing regular software patching, vulnerability scans, and back-up of data;
- performing appropriate security incident management;
- making use of data leakage prevention software, firewalls and anti-virus software;
- securing your network access points through appropriate authentication controls;
- implementing privacy policies and procedures (such as retention policies, bring your own device (BYOD) policies and clean desk policies).

However, even when reasonable and appropriate measures are taken, not all data breaches are avoidable. Accordingly, POPIA regulates the steps that must be taken in circumstances where there are reasonable grounds to believe that a data breach has occurred. In this regard, the organisation that is the "Responsible Party" must inform the Information Regulator and the person whose data has been compromised (the "Data Subject") of the data breach in the manner and form prescribed in terms of Section 22 of POPIA.

Section 22 of POPIA requires that this notification must be provided as soon as reasonably possible after the discovery of the compromise is made, 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. Section 22 of POPIA further describes the minimum information that must be provided to the data subject and the manner in which the Responsible Party may communicate the data breach to a Data Subject.

The notification to the Data Subject of a data breach may only be delayed if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator itself determines that notification will impede a criminal investigation by the public body concerned.

Third Party Breaches

Even where a Responsible Party may have watertight security measures in place, there is a risk that the third party services providers processing personal information on its behalf ("Operators") do not have appropriate and reasonable safeguards in place, which may result in a data breach. The risk escalates when the Responsible Party transfers personal information to multiple third parties (for example brokers, external marketing firms, record storage specialists or courier companies) as part of its business model.

A Responsible Party will not be absolved of responsibility in terms of POPIA on the basis that the data breach occurred at a third party level. Under POPIA, the Responsible Party will be liable where a third party (or Operator) has contravened POPIA, including where there has been an information security breach at the third party. The Responsible Party and will need to evidence that it took appropriate measures to guard against such breaches. Some steps a Responsible Party can take in this regard include conducting privacy and cyber security assessments and periodic privacy audits on third party Operators.

Section 21 of POPIA also requires the Responsible Party and Operator to enter into a written contract requiring the Operator establish and maintain the security measures that are contemplated in POPIA.

Operators are also legally required to 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 – accordingly we would expect this requirement to form part of the service level agreement between the Responsible Party and Operator.

Organisations can no longer sweep data breaches under the rug…

Now, more than ever, robust information security measures and policies must be employed by all organisations to avoid the possibility of data breaches and the potential reputational damage, financial loss, civil and criminal liability, as well as the looming penalties provided for in POPIA.

KPMG can assist you…

KPMG's multi-disciplinary team of specialists in data privacy, cyber security and technology assurance can support you in preventing, preparing for and responding to data breaches. Some of the services we provide include:

- **Third party assessments –** We can support you in identifying and assessing the privacy and IT security risks of your suppliers and third party service providers and devise a strategy to manage the privacy risk in respect of the personal data they hold or manage on behalf of your organisation.
- **Sensitive data finder service –** using a powerful data discovery tool we examine structured and unstructured data held by an organisation.
- **Cyber Defence –** Our ethical hacking specialists will help you find your organisation's vulnerabilities before the criminals do.
- **Incident Response –** We can help you prepare for cyber incidents and respond effectively when they occur through our global network of incident response

Contact our Privacy Team:

Sharmlin Moodley
Partner and member of the KPMG Privacy Team
M: +27 60 992 4789
E: sharmlin.moodley@kpmg.co.za

Marcelo Vieira
Associate Director and member of the KPMG privacy Team
M: +27 82 718 8485
E: marcelo.vieira@kpmg.co.za

Beulah Simpson
Legal Manager and member of the KPMG privacy Team
M: +27 60 602 3066
E: beulah.simpson@kpmg.co.za

Finn Elliot
Associate Director and member of the KPMG Privacy Team
M: +27 79 039 9367
E: finn.elliot@kpmg.co.za