26 JUNE 2018

TECHNOLOGY & SOURCING ALERT

IN THIS **ISSUE**

ADDRESSING YOUR DATA BREACH RISKS.....

In the wake of recent data breach incidents, it is imperative that businesses give the provisions of the Protection of Personal Information Act, No 4 of 2013 (Act) their full attention, even though the substantive provisions of the Act are not yet in force. This is borne out by the reality that these incidents are affecting South African businesses more frequently - which aligns with global statistics that point to an alarming escalation in cybercrimes and data breaches.

CDH
CLIFFE DEKKER HOFMEYR

ADDRESSING YOUR DATA BREACH RISKS.....

Even the most secure businesses could still be on the receiving end of a data breach as a result of the increasing skill and sophistication with which cybercriminals operate.

In the wake of recent data breach incidents, it is imperative that businesses give the provisions of the Protection of Personal Information Act, No 4 of 2013 (Act) their full attention, even though the substantive provisions of the Act are not yet in force. This is borne out by the reality that these incidents are affecting South African businesses more frequently - which aligns with global statistics that point to an alarming escalation in cybercrimes and data breaches.

By adopting a pro-active management strategy rather than crisis driven one and having a well-planned and comprehensive data breach response plan, you will ensure that your business is protected.

It is good business practice to ensure that your business's logical and physical security measures and safeguards are robust and are at least aligned to industry standards and where possible, to industry best practices. This is the first step to ensuring that your business is less vulnerable to a data breach or cyber incident and that your business is aligned to the requirements of the Act. The Act requires that you ensure the security and integrity of personal information in your possession or under your control with appropriate, reasonable technical and organisational measures to prevent the unlawful access to or the loss or damage or unauthorised destruction of personal information, which measures and safeguards should align to generally accepted information security practices or industry specific requirements or professional rules.

Nevertheless, even the most secure businesses could still be on the receiving end of a data breach as a result of the increasing skill and sophistication with which cybercriminals operate. This means that it is imperative to consider your risks in relation to such an eventuality and to have a robust, comprehensive data breach/cyber incident response plan in place – which can be immediately implemented should such an event affect your business.

By adopting a pro-active management strategy rather than crisis driven one and having a well-planned and comprehensive data breach response plan, you will ensure that your business is protected - not just from a legal perspective and to contain business interruption and ensure business continuity - but also from a reputational perspective. How quickly and how well you respond is a key imperative in these situations. Implementing a pre-defined data breach response plan will also assist with protecting your reputation. Timeous notification to the relevant regulators is critical and being responsive and transparent with information relating to the breach with your clients and stakeholders as well as the media can go a long way in assisting to manage the impact of a data breach on your business. The consequences of not doing so are obvious. There are numerous examples abroad of companies who had not dealt with a data breach timeously or in compliance with the law who have lost clients, share value, credibility and who suffered financially

CDH
CLIFFE DEKKER HOFMEYR

ADDRESSING YOUR DATA BREACH RISKS.....

CONTINUED

The General Data Protection Regulation (GDPR) also applies to certain South African businesses and this is already in force - so urgency is definitely the order of the day!

following a data breach (including where they have been faced with extensive investigations, damages claims and have incurred significant costs to fix the vulnerabilities in their systems).

King IV also places an obligation on the board of a company to be aware of and address the risks relating to cyber incidents. The board is tasked with overseeing business continuity and resilience arrangements as well as the business' proactive monitoring of cyber incidents. This means that cybersecurity should be a board level agenda item.

At present, the sections of the Act which have come into effect are those that establish the Information Regulator (Regulator) as the regulatory body tasked with the obligation to govern and ensure compliance under the Act, as well as the sections setting out the procedure for regulation-making by the Regulator. The chairperson of the Regulator, Pansy Tlakula, indicated in a recent radio interview that the office of the Regulator will be operational by next year. So, if this indication is anything to go by, it would appear that the remainder of the Act could come into force by next year. Even though businesses would still have a one-year grace period (which could be extended for up to three years) to become compliant with the provisions of the Act in respect of existing processing activities and it would only be then that punitive measures may be implemented against non-compliant companies, the court of public opinion is a real risk to businesses who are affected by a data breach incident. Time has run out! It is strongly advised that businesses become compliant with the requirements of the Act and it does not stop there. To fully protect your business and ensure that you do not cause unnecessary damage to your reputation or at least are effective at mitigating the fall out of any serious data breach impacting your business, you should plan for such an eventuality.

The General Data Protection Regulation (GDPR) also applies to certain South African businesses and this is already in force - so urgency is definitely the order of the day!

Preeta Bhagattjee

OUR TEAM

For more information about our Technology & Sourcing practice and services, please contact:

Christoff Pienaar
National Practice Head
Director
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Preeta Bhagattjee
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@cdhlegal.com

Simone Dickson
Director
T +27 (0)11 562 1249
E simone.dickson@cdhlegal.com

Vania Munro
Director
T +27 (0)21 481 6345
E vania.munro@cdhlegal.com

Fatima Ameer-Mia
Senior Associate
T +27 (0)21 481 6374
E fatima.ameermia@cdhlegal.com

Bilal Bokhari
Associate
T +27 (0)11 562 1589
E bilal.bokhari@cdhlegal.com

Aphindile Govuza
Associate
T +27 (0)11 562 1090
E aphindile.govuza@cdhlegal.com

JOHANNESBURG

1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa. Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN

11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com