13 FEBRUARY 2019

TECHNOLOGY & SOURCING ALERT

IN THIS **ISSUE**

CYBERCRIMES BILL – A POSITIVE STEP TOWARDS THE REGULATION OF CYBERCRIMES IN SOUTH AFRICA

Technology has become an indispensable part of modern life – it has significantly changed the way people communicate and do business. In a world and country where technology is dynamic in nature and is continuously evolving, South Africa has struggled to keep up with these developments and in regulating cyber security and cybercrimes.

THE CURIOUS CASE OF CONSENT: GOOGLE FINED 50 MILLION EURO FOR BREACHING THE GDPR

French Data Regulator, Commission Nationale de l'Informatique et des Libertés (CNIL'), recently fined Google 50 million euro for breaching the provisions of the General Data Protection Regulation ('GDPR') which came into effect on 25 May 2018. This follows complaints brought by consumer organisations None of Your Business and La Quadrature Net against the tech giant in 2018.

FOR MORE INSIGHT INTO OUR EXPERTISE AND SERVICES

CLICK HERE

CDH
CLIFFE DEKKER HOFMEYR

CYBERCRIMES BILL – A POSITIVE STEP TOWARDS THE REGULATION OF CYBERCRIMES IN SOUTH AFRICA

At present, the current legal framework relating to cybercrime in South Africa is a hybrid of different pieces of legislation and the common law which has not kept up with the dynamic nature of technology and international standards.

Technology has become an indispensable part of modern life – it has significantly changed the way people communicate and do business. In a world and country where technology is dynamic in nature and is continuously evolving, South Africa has struggled to keep up with these developments and in regulating cyber security and cybercrimes.

Cyber-related incidents such as cybercrimes, IT related failures and data breaches have been rated as the number one risk to South African businesses according to the 2018 Allianz Risk Barometer report. South Africa is further a top target for cybercrime in Africa because of its high internet connectivity rates, attractive GDP per capita and poor levels of cyber security (especially in business).

At present, the current legal framework relating to cybercrime in South Africa is a hybrid of different pieces of legislation and the common law which has not kept up with the dynamic nature of technology and international standards. This prompted the need for the Cybercrimes Bill, which will, *inter alia*, consolidate and codify numerous existing offences relating to cybercrime as well as create a variety of new offences which do not currently exist in South African law.

The Old Bill was divided broadly into two parts, namely cybercrimes and cybersecurity.

Old Bill vs New Bill

It is important to note that the version of the Cybercrimes Bill which was passed by the National Assembly in November 2018 (New Bill) differs quite substantially from the versions of the Bill published previously (Old Bill).

The Old Bill was divided broadly into two parts, namely cybercrimes and cybersecurity. The cybercrimes section, bar a few criticisms, was lauded however it was the proposed cybersecurity section which raised very serious concerns about the government's encroachment on freedom of expression and freedom of the internet. It was argued that the Bill's approach did not strike the right balance between the interest of the State in securing cyberspace and individual freedoms and rights.

CDH
CLIFFE DEKKER HOFMEYR

CYBERCRIMES BILL – A POSITIVE STEP TOWARDS THE REGULATION OF CYBERCRIMES IN SOUTH AFRICA

CONTINUED

It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the Electronic Communications and Transactions Act, No 25 of 2002 relating to cybercrime offences.

However, given the urgent need for legislation that comprehensively criminalises cybercrime, the Portfolio Committee on Justice and Correctional Services have decided to strip out all clauses in the Bill pertaining to cybersecurity and to proceed only with cyber related crimes.

What are the key clauses to watch for in the New Bill?

The New Bill now specifically only 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.

Some of the key clauses relate to:

- the new offences which have been created under the Bill (which were previously difficult to prosecute) such as the distribution of a data message of an intimate image (often referred to as the "revenge-porn" offence), the infringement of copyright (through the use of "peer-to-peer" sharing), offences relating to malicious communications by disseminating a data message which advocates, promotes or incites hate, discrimination or violence against a person or group of persons;
- the jurisdiction clauses which are more extensive and allow for South African courts to have extraterritorial jurisdiction even where offences are committed outside of South Africa (in certain instances);
- the penalty provisions which provide for a maximum penalty (depending on the offence) of up to 15 years imprisonment or to both a fine and imprisonment; and
- the obligations placed on electronic communications service providers and financial institutions which becomes aware that its computer system was involved in the commission of an offence to within 72 hours report the offence in the prescribed form to SAPS and preserve any evidence related to the offence.

It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the Electronic Communications and Transactions Act, No 25 of 2002 relating to cybercrime offences.

What are their implications for businesses?

With regards to the reporting and preservation of evidence requirements placed on electronic communications service providers and financial institutions, failure to comply with the Bill will render such business liable for an offence and fine up to R50,000. These obligations may also result in increased costs and losses to companies in the event of a cybercrime occurring. If computer equipment is confiscated or seized (for long periods of time rendering them inaccessible) by the relevant authority to investigate a crime or preserve evidence, it will also result in an increased cost to business and may result in business interruption.

CDH
CLIFFE DEKKER HOFMEYR

CYBERCRIMES BILL – A POSITIVE STEP TOWARDS THE REGULATION OF CYBERCRIMES IN SOUTH AFRICA

CONTINUED

The Trend Micro Report notes that 2019 will be an important year for political developments including Brexit and national elections in several countries, including South Africa.

Trend Micro released a report in December 2018 outlining its security predictions for 2019 (Trend Micro Report). The Trend Micro Report predicts that the biggest trends expected to have an impact on technology and security are:

- the advances in artificial intelligence and machine learning brought about by the ever-growing volume of data that can be processed and analysed;
- the continued adoption of cloud computing by enterprises the worked over;
- and the developments in smart devices, homes and factories.

Further, the Trend Micro Report notes that 2019 will be an important year for political developments including Brexit and national elections in several countries, including South Africa. These technological and socio-political changes are predicted to have a direct impact on security issues in 2019.

In this regard, the Cybercrime Bill and the global trend of increased cyber regulations may be the impetus for companies to consider cyber risk insurance cover to preserve their economic welfare. Businesses should therefore start prioritisinginformation security and assessing their levels of risks and exposure.

In particular, businesses should consider formulating a cyber incident response plan which includes establishing notification and escalation procedures when a cyber incident occurs, formulating a PR strategy in the event of an incident, establishing evidence gathering guidelines, and a stakeholder notification procedure (including any regulatory authorities).

It is also worth noting that the final Regulations to the Protection of Personal Information Act (POPI) were published in December 2018. These will come into force once the commencement date of POPI has been proclaimed by the President.

The fact that the legislature has taken active steps towards prioritising these pieces of legislation is a positive development and it remains to be seen whether we will see the Cybercrimes Bill and POPI being enacted during the current legislature's tenure. Businesses should therefore start adopting a pro-active approach to compliance and implement a risk management framework to ensure it is adequately prepared in the event of a cyber-attack. This includes prioritising the security of their data and IT systems.

Fatima Ameer-Mia and Lee Shacksnovis

CDH
CLIFFE DEKKER HOFMEYR

THE CURIOUS CASE OF CONSENT: GOOGLE FINED 50 MILLION EURO FOR BREACHING THE GDPR

Google failed to provide transparent and easily accessible information to users relating to its data consent policies, particularly how personal data is used with regard to personalised advertisements.

French Data Regulator, Commission Nationale de l'Informatique et des Libertés (CNIL'), recently fined Google 50 million euro for breaching the provisions of the General Data Protection Regulation ('GDPR') which came into effect on 25 May 2018. This follows complaints brought by consumer organisations None of Your Business and La Quadrature Net against the tech giant in 2018.

It did not obtain sufficient and specific consent from users for personalised advertisements across its services.

The complaints concerned Google's consent practices when users create a Google account. When creating an account, users are required to agree to Google's terms of use, privacy policy and data collection process by scrolling through the page using the ''*more*'' button. By doing this, users are deemed to have given the necessary consent to Google for the collection of their personal data and to receive personalised advertisements.

The CNIL held that, by requiring users to do this, Google failed to comply with two provisions of the GDPR. Firstly, it failed to provide transparent and easily accessible information to users relating to its data consent policies, particularly how personal data is used with regard to personalised advertisements. Secondly, it did not obtain sufficient and specific consent from users for personalised advertisements across its services.

What should be made clear is that the terms of use and privacy policy information are available, however, neither are easily accessible. Users have to scroll through various settings and options to access this information. In addition, it is not that users do not consent to Google's policies, but rather that users' consent is not fully informed. Users therefore do not fully understand the extent to which their personal data will be used for personalised advertisements across all Google's services. The CNIL held that the consents collected by Google are ambiguous and not specific to each of its various services, which are offered across many different platforms and devices. Further, the option for personalised advertisements is already pre-ticked when users accept Google's data policies. Unless users know that the option of personalised advertisements is already pre-ticked and can navigate their way to the options and settings, they cannot turn it off.

Article 4(11) of the GDPR outlines the criteria for consent as follows:

> [C]onsent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.''

CDH
CLIFFE DEKKER HOFMEYR

THE CURIOUS CASE OF CONSENT: GOOGLE FINED 50 MILLION EURO FOR BREACHING THE GDPR

CONTINUED

This case serves as a clear indication to all companies to comply with the provisions of the GDPR whether they consent to them or not.

In Google's case, users are requested to consent to a wide range of services with a single action and therefore the consent requested is not specific. To comply with the GDPR, Google must require consent for each of its services. Furthermore, Google's data collection process needs to be clear and easy to understand, particularly as it can reveal significant aspects of a user's private life.

The GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action, prohibiting the use of pre-ticked and opt-in boxes. Therefore, Google must update its consent gathering mechanisms by offering unticked boxes to allow users the option to consent to a specific service.

It is interesting to note that Google has announced that it is appealing the CNIL's decision, which should provide further clarity on how the GDPR must be applied in practical situations. Irrespective of the outcome of the appeal, this case serves as a clear indication to all companies to comply with the provisions of the GDPR whether they consent to them or not.

Written by Cyprian Mthembu, overseen by Simone Dickson and Preeta Bhagattjee.

CDH
CLIFFE DEKKER HOFMEYR

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

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

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

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

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