ANNUAL CONFERENCE OF THE AFRICAN BAR ASSOCIATION

NAIROBI, KENYA, JULY 22 – 27 2018

Conference Theme: "Africa's Socio-Economic and Political Future: Africa Union's Agenda 2063 in perspective"

Sub -Theme: "Media, Privacy and Data Protection: How helpful is Africa's Information Strategy"

Paper Topic: "Technological change and globalisation of businesses –Data Security, Risks and Privacy"

Presenter: James M. Derby. (Solicitor of England and Wales)

Introduction

At any legal conference, delegates will consist mainly of lawyers from 3 or 4 sectors i.e. private practice, in-house, public sector and voluntary sector. A good presentation at any legal conference will ensure issues in the paper affecting all delegates are considered, addressed and action points recommended. This paper will seek to do all these.

With the advancement of technological innovation and cross-border trade, compliance with international personal data protection legislation and standards has become imperative. This is due to the fact that non-compliance with personal data protection legislation could impede an organisation from transferring personal data cross-border, thereby hindering its business operations. This is particularly relevant for multinational organisations with a global footprint who transfer personal data cross-border in the ordinary course of business in conducting international trade.

Let me be very clear from the start, I believe that the internet and the new generation of digital communications and digital platforms offer immense possibilities to each and everyone of us in our socio-economic and political lives. In terms of choice, access and opportunity, they are some of the most empowering tools we have ever had. I am convinced that new information and communication technologies will bring enormous benefits to the entire world.

Africa has a long and chequered history about privacy rights; citizens constantly face the challenge about their rights to privacy; media houses are constantly facing the right to freedom of the press, the advancement of technological innovations including the power of social media has changed the trajectory of living and doing business. This paper will address in detail, privacy and data issues affecting the Africa continent vis a vis its Information Management Strategy and aligning it to the global standards in a digitally disruptive age of the internet and electronic commerce (e-commerce) involving the cross-border flow of data.

Issues to be considered in the paper:

- the current African personal data protection regulatory landscape; Benchmark with the EU General Data Protection Regulation (GDPR) and Privacy laws in the USA
- the compliance challenges which this regulatory landscape precipitates for organisations with an African footprint seeking to leverage off the vast investment opportunities in Africa; and
- how organisations may potentially overcome pertinent personal data protection regulatory obstacles, while concurrently augmenting business growth, stakeholder confidence and market competitiveness.

Details

Business in Africa is expanding at a rapid pace due to a proliferation of investment opportunities on the continent. To effectively conduct business in Africa, organisations need to understand the African personal data protection regulatory landscape. The importance of data has recently being highlighted by the allegation that Cambridge Analytica, a UK data analysis firm used data from Facebook to help US President Donald Trump get elected and to assist the Brexit campaign group Leave.EU win the EU referendum elections in UK.

If Britain hadn't voted to leave the EU, and Trump hadn't won the US election, it's unlikely anyone outside Nigeria would have given a second thought to what went on during its presidential election campaign three years ago. At the heart of the 2015 general elections in Nigeria– data analytics company, SCL – the parent company of Cambridge Analytica was purportedly hired by a supporter of the then incumbent, President Goodluck Jonathan. According to The Guardian (UK) online of 21 March 2018 "seven individuals with close knowledge of the Nigeria campaign have described how Cambridge Analytica worked with people they believed were Israeli computer hackers. The sources – who spoke to the Observer

over many months – said the company was looking for "kompromat" on Muhammadu Buhari – at the time, leader of the opposition……..The company (SCL) confirmed, however, that it had been hired to provide "advertising and marketing services in support of the Goodluck Jonathan campaign".

The theme of the paper revolves round the word data in relation to data protection. Privacy lawyers, practitioners, and legislations use the word data interchangeably with the words personal data or personal information. The logical question therefore is what is data?

According to Meglena Kuneva, European Consumer Commissioner "Personal data is the new oil of the internet and the new currency of the digital world"[1]. In 2006, Clive Humby, the UK Mathematician and architect of Tesco's Clubcard stated "Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value."

Africa's biggest trade partners are still in Europe and America despite the progress made with trade relations with the Near and Middle East and Asia. The European Union (EU) countries have had data protection legislations since 1995 and from 25 May 2018, the EU now has a common data protection Regulation known as the General Data Protection Regulation (GDPR).

USA

"In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. However, each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not

[1] . Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling Brussels, 31 March 2009

have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.

There are many laws at the state level that regulate the collection and use of personal data, and the number grows each year. Some federal privacy laws pre-empt state privacy laws on the same topic. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses pre-empts most state laws regulating the same activities. Conversely, there are many federal privacy laws that do not pre-empt state laws, which means that a company can find itself in the position of trying to comply with federal and state privacy laws that regulate the same types of data (for example, medical or health records) or types of activity.
Most states have enacted some form of privacy legislation, however California leads the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level.
California was the first state to enact a security breach notification law (California Civil Code §1798.82). The law requires any person or business that owns or licenses computerised data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorised person"[2]

Africa

Unlike the EU, Africa as a continent has no unified approach to personal data protection across the continent however, the privacy landscape in Africa has changed over the last

[2] Ieuan Jolly, Loeb & Loeb – Thompson Reuters, Practical law

decade. Currently, 17 African countries have comprehensive personal data protection legislations in place and others have no legislation or constitutional protection. The Countries with data protection legislations are: Angola, Benin, Burkina Faso, Cape Verde, Chad, Coˆte d'Ivoire, Equatorial Guinea, Gabon, Ghana, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, South Africa and Tunisia. In fact, there are indications that countries such as Kenya, Niger, Tanzania, Uganda, and Zimbabwe may be close to adopting their privacy legislations.

In June 2014, the African Union (AU), adopted the AU Convention on Cybersecurity and Data Protection (AU Convention). However, the AU Convention has not currently taken effect as it has, to date, not been ratified by the required 15 out of the 54 AU member jurisdictions; Only two countries have ratified it, they are: Senegal on 3rd August 2016.and Mauritius on 6th March 2018. Nonetheless, the AU Convention does provide a personal data protection framework which African countries may potentially transpose into their national legislation, and encourages African countries to recognise the need for protecting personal data and promoting the free flow of such personal data, taking global digitalisation and trade into account[3]

The AU Convention defines personal data as "any information relating to an identified or identifiable natural person by which this person can be identified directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/ her physical, physiological, mental, economic, cultural or social identity"[4]

Article 4 of the GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be

[3] African Union Convention on Cyber Security and Personal Data Protection. 14/03/2018
[4] Ibid 2

identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[5]

From the above definitions data protection is about the 'protection of privacy rights and freedoms of natural persons but further their right to the protection or personal data"[6]. We now live in a world of technological advancement. The GDPR has taken into consideration the impact of technology in this digitally disruptive age of the internet and electronic commerce (e-commerce) involving the cross-border flow of personal data. A high premium has therefore been placed on personal data and its ability to either promote or hinder international trade.

The hallmark of any data protection legislation includes provision for a national agency responsible for enforcement of the legislation; this is generally known as the Data Protection Authority (DPA). The agency though a creation of statute should be an independent body. The data protection legislation should provide inter alia for the roles and responsibilities of the DPA, the rights of individuals (data subjects) such as right of access to information held about an individual, Choice and Consent, Privacy Notice, Right of Rectification, Data Security, Data Retention and Deletion, cross border transfer of data, exemptions to these rights (e.g. national security, prevent of crime, apprehension and prosecution of offenders), and a robust enforcement regime (e.g. independent investigation, monitoring and audit and fines).

[5] eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
[6] Ibid 4 (Article 1)

A good data protection legislation should also provide for registration with the regulator, the appointment by each organisation "processing" data of a Data Protection Officer (DPO), and a data breach notification requirement.

An effective national regulator (DPA) operates as the "Police" of the legislation. Under the GDPR all Member states have a regulator e.g. in UK it is the Information Commissioner's Office (ICO). In Africa, several of the countries with a national privacy legislation are still in their formative stages, in large part because the regulators are either not yet in place or have been recently appointed and/or have insufficient funding; however, in some of the countries with the more established privacy regimes, the regulators have been stepping up their enforcement efforts.

The Enforcement of personal data regime in Africa is still at a very embryonic stage, however, "Enforcement activity in the region continues to grow. In addition to the data protection authorities (DPAs) in Mauritius, and Morocco, who have well-established programs, the DPAs in Benin, Ghana, Mali, Senegal, and Tunisia are becoming more outspoken and active. In February 2017, the Mali DPA fined a telecommunications company 15 million CFA francs ($27,457) for violating its security obligations under the Mali data protection law, which resulted in unauthorized access to a customer's cellphone messages by a company employee. The year before, it fined two utility companies 5 million CFA francs ($9,152) each for violating their security and confidentiality requirements under the Mali law. The companies were found to have unlawfully publicized on social media the electricity and water bills of delinquent clients. In Senegal, the DPA has been carrying out inspections in response to complaints, identifying law violations, and issuing recommendations. The DPA has announced its intention to pay particular attention to cross-border transfers to make sure

they comply with the requirements under the law. It also has encouraged citizens to report any law violations to the DPA or simply check and challenge the legality of the processing of their personal information. In Tunisia, the DPA, which generally does not publish information about its enforcement actions, announced last year that it would be filing lawsuits against 12 public and private organizations for privacy law violations. In Ghana, the DPA is going after data controllers who have failed to register their processing activities. The registration process began on May 1, 2015, and organizations were given six months to file their registrations. As of early this year, only a minority of data controllers had registered. After issuing verbal warnings to more than 100 organizations in 2016, the DPA is now working with the police to make sure those who fail to register are sanctioned accordingly. In March 2017, the DPA reported that three organizations had been convicted of violating the law and fined for failing to register, but no specific details regarding those fines were provided. Also noteworthy is the creation last year of the African Network of Personal Data Protection Authorities (RAPDP) by Cape Verde, Benin, Burkina Faso, Cote d'Ivoire, Mali, Morocco, Senegal, and Tunisia. The purpose of the RAPDP is to organize close cooperation between

members, support the drafting of data protection laws, formulate opinions or statements on specific issues, establish a consultative framework on data protection issues and challenges, and promote African data protection instruments. Increased cooperation among these African regulators is likely to encourage other authorities in the region to step up their own enforcement efforts"[7]

There is a clear indication that the datafication of personal information will continue to be fostered by powerful companies, resulting in a data imbalance between the data haves

[7] Cynthia Rich. A Look at New Trends in 2017: Privacy Laws in Africa and the Near East

(government and large corporations) and have nots. Furthermore, the very asymmetry of power around who controls personal data is fostering practices such as data commodification, identity theft, surveillance, and profiling, which are putting the lives of individuals at risk. In the EU the GDPR will give people better privacy protections and force companies including Facebook and Google to make sweeping changes to the way they collect data and consent from users – with huge fines for those who don't comply. Notably, the current fine regime from the EU regulators for serious breaches of personal data which stood at a maximum of £500,000.00 has under GDPR increased to a maximum of £17,000,000.00 or €20,000,000.00 or 4% of annual turnover. In the UK, the Information Commissioner's Office has awarded fines against various organisations (including private, public and voluntary) such as Crown Prosecution Service (£325,000.00), Yahoo UK Services Ltd (£250,000.00), Humberside Police (£130,000.00) and University of Greenwich (£120,000.00)[8]

In Africa, collection or "processing" of personal data will continue on a large scale mainly by Governments regulated institutions or organisations providing services. Government "processes" data through institutions such as Immigration services, passport offices, tax offices. Regulated institutions such as Banks and Insurance companies also "process" data. Hospitals (both private and public) are major processors of personal and sensitive personal data; corporations such as phone companies, airlines and educational institutions "process" data when customers register for services and their data such as personal information, biometrics and passport details are collected before services can be offered to them.

[8] www.ico.org.uk

Compliance challenges

Despite the positive steps highlighted above about enforcement activities the data protection regime in Africa still faces severe compliance challenges; the main challenge being insufficient funding for the regulator (if any), respect for the rule of law, lack of or non-compliance with governance processes, ineffective enforcement regime and lack of organisational or technical measures to prevent unlawful or unauthorised processing of personal data

For African companies doing business within the European Union, or oriented towards the European Union, it is important they acquaint themselves of the GDPR, whether they process personal data related to persons located within the EU for their own purposes, or whether they provide services to European companies or public bodies. For such African organisations a lack of compliance with the GDPR would entail two types of risks, namely commercial and legal risks. On one hand, there are risks of a commercial nature, if a compliant level of protection is not sufficiently guaranteed, especially concerning security and confidentiality of personal data, European companies or public bodies would be entitled to break the contract at stake. Moreover, in the context of a bid solicitation or of a competitive call, the lack of proof or guarantee of compliance with the GDPR would necessarily lead to the loss of any chance to win the concerned market or project.

On the other hand, there are legal risks, for the GDPR provides a shared liability between controllers and processors. In case of infringement, both of them will be subject to heavy administrative or even criminal penalties. It is therefore crucial that African processors working for European companies or public bodies limit their risks of liability, as well as any African company processing personal data related to persons located within the EU for its own purposes.

It must also be reminded that the GDPR prohibits any transfer of personal data outside of the EU, except for a few limited exceptions, if an adequate level of protection, equivalent to the level set by European law, is not guaranteed. African companies which intend to keep on receiving data from their European partners will therefore have to provide sufficient guarantees of such an adequate level of protection.

Some companies are concerned as “data processors”. Those are companies which, in a context of provision of services to European companies or public bodies, process personal data related to employees, customers, users or other providers, or to any natural person living within the EU. Such companies are in particular computer or consulting service providers, like audit, computer or user rescue plans, hotline services or call centers. Such may also provide outsourcing operations of whole branches of the activity of European companies or public bodies. Some other companies are concerned as “data controllers”. Those are companies which determine by themselves the purposes and means of their own personal data processing, if this processing is related to persons located within the EU, for the purpose of providing them goods or services, or for profiling purposes. Such companies are in particular e-commerce companies which sell goods to customers located within the EU, and which edit and manage customer files for that purpose.

Overcoming data protection regulatory obstacles

The major benefits of data processing include easy access to services, national security, apprehension and prosecution of offenders, access to global investment opportunities, mechanism for protecting privacy particularly in a digital age especially some non-negotiable

rights such as right of access to information and right to know how your information is being used. Of particular interest is the potential for global business opportunities which processing of data presents to Africa. For example, in UK, organisations including private, public and voluntary sectors now explore the opportunities to enter into various legal arrangements with companies in India for processing of data of UK citizens as a result of availability of technological know-how and reasonable costs. These business models are supported by legal arrangements and protected through adequate safeguards such as "model clauses" and "Binding Corporate Rules" (BCRs). In the US, the Privacy Shield provide adequate level of protection for cross border transfer of data between the EU and US.

In order for African countries to overcome various data protection regulatory obstacles they must have robust data protection legislation and as a matter of priority provide sufficient funding for their data protection regulatory agencies: the agencies must be independent and free from any influence or control by Government; the agencies must be well staffed and employees well trained, there should be robust policies, processes, procedures and governance structures available to support the various roles of the regulatory agency.

According to Deloitte "if the GDPR standard – considered to be among the highest global personal data protection standards – were to be applied by multinational organisations with an African footprint, this would ensure compliance with most, if not all African personal data protection requirements"[9]. It is therefore advisable that the GDPR be used as baseline for data protection legislations in Africa. Further African countries must through relevant data protection legislation ensure organisations processing personal information either as a data

[9] Deloitte = Privacy is Paramount Personal Data Protection in Africa (2017)

controller[10] or data processor[11] have adequate level of security for data. This will include technical and organisational measures which meet international standards.

Data protection regulatory obstacles will also be overcome where the data protection regulatory authority has sufficient and effective regulatory and enforcement powers; this will include the role of investigating non-compliance with the data protection regulation, investigation of breaches of the regulation and where appropriate carrying out enforcement actions such as data protection audit of the organisation, monitoring an organisation's information rights practices and issuing monetary fines.

Conclusion

In conclusion, respective African Governments must take more interest towards the issues relating to privacy rights; at the least, African countries can start with ratification of the AU Convention on Cybersecurity and Data Protection. Governments, organisations and multinationals in Africa should proactively embed in their corporate policies a robust data protection regime as done by international organisations such as the World Bank, UN and IMF, and protect the privacy rights of its employees. The EU through the GDPR is taking further steps to protect the privacy of its citizens and offer more rights and transparency; African countries should also aim towards these practices.

Ultimately a robust data protection regime within African countries would provide assurances to investors across the globe ensuring that they are able to effectively capitalise or leverage on the vast investment opportunities in Africa, "as personal data is the new currency with which to effectively conduct business operations globally"[12]

Thank you for listening.

[10] As defined in Section 3 of the Data Protection Act 2018 (UK)
[11] Ibid 9
[12] Ibid 8