Deloitte.

Privacy is Paramount

Personal Data Protection in Africa

The importance of compliance with personal data protection legislation for business growth and international trade

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. Personal data protection legislation may potentially restrict a multinational organisation's ability to conduct international business trade if compliance is inadequate. Whether or not an organisation is being prevented from transferring personal data cross-border, is an issue of data sovereignty, in addition to being a data protection issue. Data sovereignty is the principle that data, especially in electronic form, is regulated by the laws of the country in which such data resides. Personal data protection laws contain data sovereignty principles in that they prevent the transfer of personal data to another country, unless certain conditions for such transfer are complied with under the laws of the country from which the personal data transfer is to be made.

In the digitally disruptive age of the internet and electronic commerce (e-commerce) involving the cross-border flow of personal data, a high premium has been placed on personal data and its ability to either promote or hinder international trade. Hence, e-commerce has ushered in a new era of international trade, particularly on the resource-rich African continent, where business growth and foreign direct investment continually allow the harnessing of new opportunities.

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. Non-compliance with personal data protection legislation in Africa may potentially preclude multinational organisations from capitalising on their African exploits, by restricting their ability to transfer personal data to third parties beyond African borders, thus hindering business operations.

In order for multinational organisations to facilitate the cross-border transfer of personal data between their various geographical operations and optimise their business processes in Africa, we set out the following:

- the current African personal data protection regulatory landscape;
- the compliance challenges which this regulatory landscape precipitates for multinational organisations with an African footprint seeking to leverage off the vast investment opportunities in Africa; and
- how multinational organisations may potentially overcome pertinent personal data protection regulatory obstacles, while concurrently augmenting business growth, stakeholder confidence and market competitiveness.

A core theme with regard to international trade and personal data protection regulatory compliance, is the issue of cross-border personal data transfers, which are necessary in order for global organisations to conduct business internationally. As will be discussed further in this whitepaper, African personal data protection laws (in the African countries where they do exist) place restrictions on the transfer of personal data to third parties who are situated outside the borders of the country in which an organisation has a presence, and from which the personal data is being transferred.

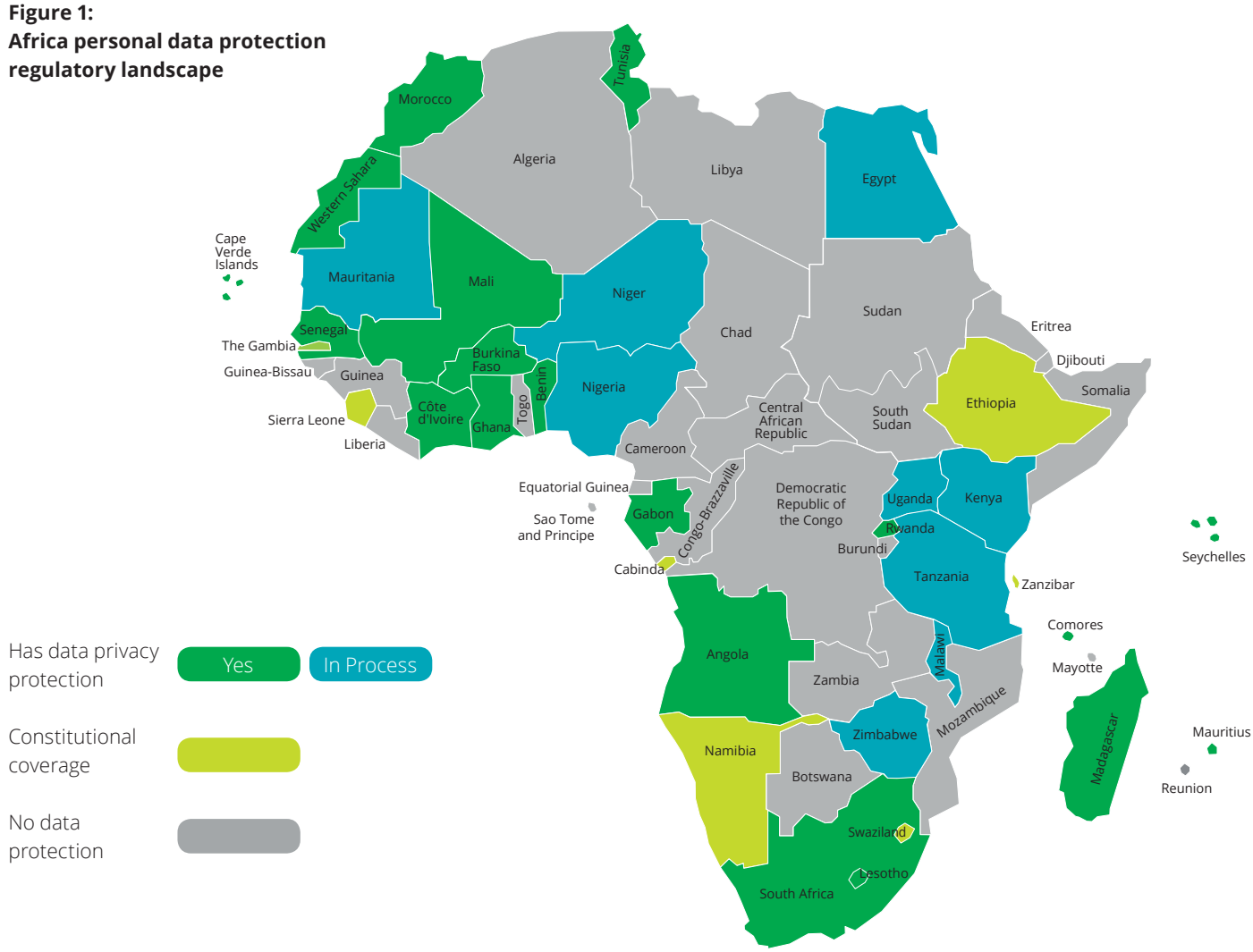
However, these restrictions are not intended to be a barrier to organisations' African (and global) business operations. Rather, they outline the conditions which must be fulfilled for cross-border personal data transfers to be within the limits of the relevant African personal data protection legislation. In the event that these laws are not complied with, organisations would not be able to lawfully transfer personal data (whether relating to customers, employees, suppliers, business partners or others) across borders as part of their business operations. This could potentially result in lost business opportunities and hamper an organisation's ability to trade internationally, leading to a diminished geographical footprint which in turn, could result in reduced revenues and market competitiveness.

An example of the above issue is that of cloud technology and cloud-based solutions, which seek to improve a multinational organisation's efficiency and make its data (including personal data) instantly available all over the world. This would ultimately entail the cross-border transfer of personal data, firstly, to the cloud provider's data centres (should they not be located in the same country as the organisation i.e. offshore), and secondly, to the geographic locations from which the data will be accessible (by anyone within the organisation from any location). A multinational organisation would have to ensure that it engages a cloud provider whose data servers are located in a country with adequate personal data protection laws, especially if such data is to be stored on the African continent. Africa for the most part, does not have personal data protection law, save for a few countries (to be discussed).

Understanding the African personal data protection landscape

In Figure 1 below, we provide an outline of the personal data protection coverage in Africa. As is evident from the diagram, there is no unified approach to personal data protection across the African continent, with some countries having comprehensive personal data protection legislation in place and others have no legislation or constitutional protection. Adapting personal data compliance programmes to be in line with disparate legislation and regulation is no minor feat.

Figure 1:
Africa personal data protection regulatory landscape



There are currently 17 countries in Africa that have enacted comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara[1]. In addition, the African Union (AU), adopted the AU Convention on Cybersecurity and Data Protection (AU Convention) in June 2014[2]. However, the AU Convention has not currently taken effect as it has, to date, not been ratified by 15 out of the 54 AU member jurisdictions[3]. 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[4]. In this regard, there are three countries, namely Kenya, Uganda and Zimbabwe, which have already enacted personal data protection legislation, the promulgation of which has not yet been made effective, as the laws are still in the form of bills. Tanzania is another country which is currently in the process of enacting personal data protection legislation[5].

Comparison with the European Union Personal Data Protection Regulatory Framework

We have noted the EU personal data protection position here for comparative purposes as far as the AU Convention and the African personal data protection regulatory framework is concerned. We have also highlighted the EU position with a view to demonstrate the benefit to organisations in developing and implementing a comprehensive compliance programme for their African personal data protection regulatory framework – similar to that which would be developed and implemented in respect of organisations' EU operations, if any.

The European Union (EU) General Data Protection Regulation (GDPR), which will officially come into force on 25 May 2018, will replace the current Data Protection Directive 95/46/ec (the Directive). The difference between the GDPR and the Directive is that, unlike the Directive, the GDPR is automatically enforceable within EU member states and does not, in contrast to the Directive, have to be transposed into EU member state legislation. Hence, it can be said that the AU Convention is similar to the Directive, in that the AU Convention will not have any legal force unless it is transposed into an African country's legislation. Furthermore, the EU is similar to Africa in the sense that there are disparate data protection legislative requirements across the various EU member states, which can present unique compliance challenges to organisations with an EU presence. Thus, the GDPR will unify the EU's personal data protection regime, thereby making it somewhat simpler for organisations with an EU presence (throughout several EU member states) to streamline their compliance activities across their EU footprint. It is easier to comply with a single piece of personal data protection legislation across multiple EU jurisdictions, as opposed to several disparate pieces of legislation within the region.

Along these same lines, it is elucidated further below, how organisations with an African presence may conduct their personal data protection compliance programmes to achieve adequate compliance with disparate Africa legislative regimes – in light of Africa and its AU Convention not currently having a "GDPR-equivalent" personal data protection framework in place.

There are common personal data protection themes or principles contained in the legislation adopted by the African jurisdictions which have enacted comprehensive data protection legislation[6]. These themes comprise:-

- notice
- choice and consent
- data security
- data access and correction
- data quality and integrity
- data retention and destruction
- registration with a data protection authority (DPA)
- cross-border data transfers
- personal data breach notification
- appointment of a data protection officer (DPO)[7]

1. Cynthia Rich (2016) Privacy Laws in Africa and the Near East (16) 6 *Bloomberg BNA World Data Protection Report*, 1
2. Ibid 1
3. Ibid 4
4. Ibid 1, 4
5. Ibid 2
6. Ibid 2
7. Ibid 2

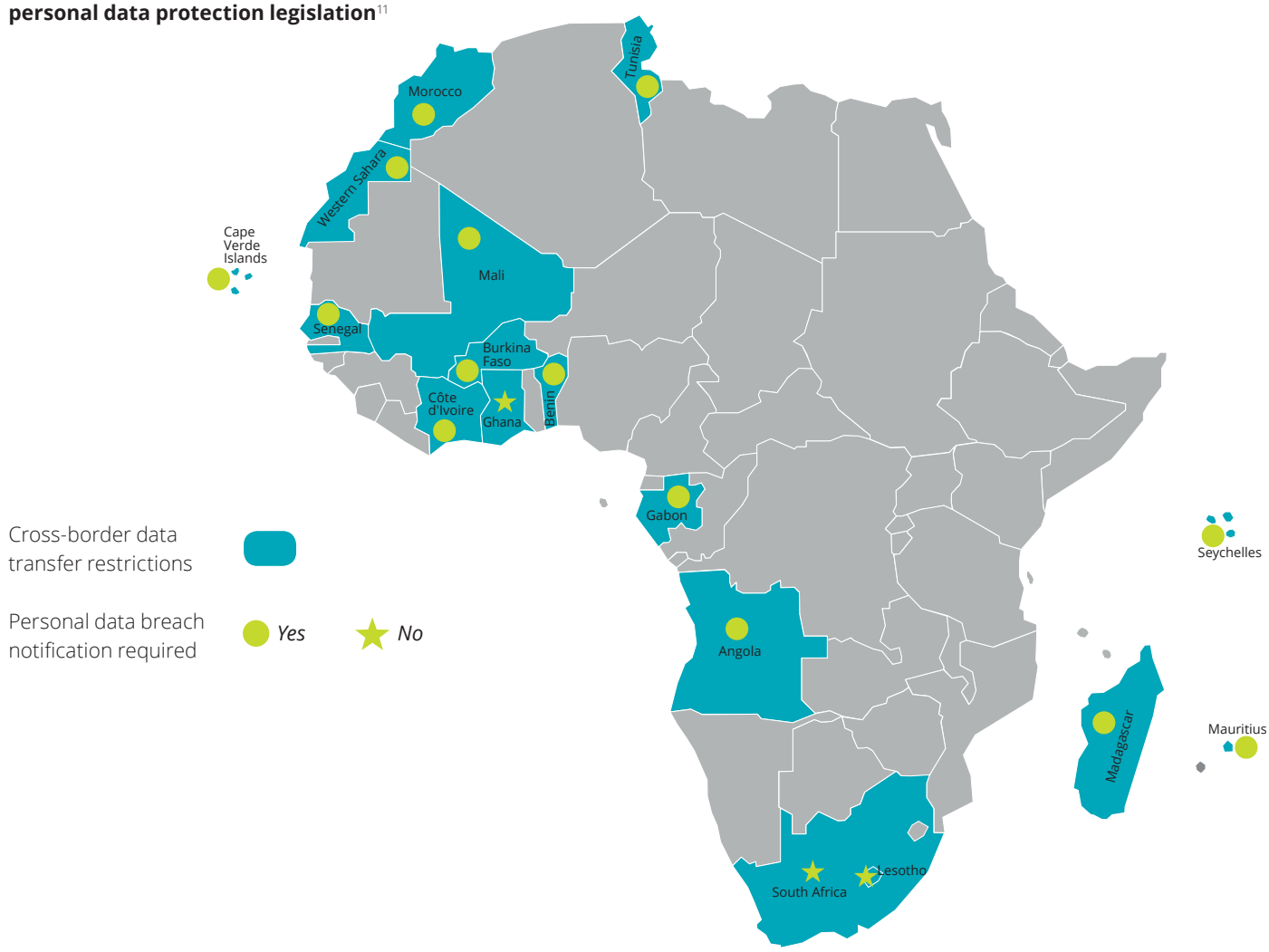
Despite most of the aforesaid personal data protection themes being contained in the legislation adopted by the above-mentioned African countries, there are particular principles that differ significantly from country to country. The pertinent personal data protection principles to which these differences relate, are:

- registration with a DPA
- cross-border data transfers
- data breach notification
- appointment of a DPO[8].

In this regard, while some jurisdictions require organisations to register with a DPA, others do not. Moreover, 15 of the 16 above-mentioned African countries require that organisations put in place mechanisms for the cross-border transfer of personal data[9]. The legislative disparities between the various African jurisdictions in respect of personal data protection may prove challenging to multinational organisations with an African presence. Accordingly, any compliance programmes will need to be tailored to account for these disparities. Lack of compliance will result in stiff penalties if all legislative nuances are not sufficiently addressed[10].

The diagram below (Figure 2) is demonstrative of such challenges:

Figure 2:
Cross-border data transfer and breach notification requirement in African countries which have adopted personal data protection legislation[11]



8. Ibid 2
9. Ibid 2
10. Ibid 2-3
11. Cynthia Rich (2016) Privacy Laws in Africa and the Near East (16) 6 *Bloomberg BNA World Data Protection Report*

It is evident from Figure 2 that while organisations with a presence in any of the above African jurisdictions will need to ensure that it has cross-border mechanisms in place within each relevant jurisdiction, it only needs to implement breach notification mechanisms within its business processes where it has a presence in Ghana and South Africa. However, international personal data protection best practice dictates that despite breach notification mechanisms not being required in all other jurisdictions, it is nonetheless imperative for organisations who have suffered a personal data breach, to notify affected individuals that their personal data may have been compromised.

Existing Trends and Aggressiveness of African DPAs in enforcing personal data protection legislation

Current statistics reflect DPA activity in countries such as Ghana and Mauritius as being more robust due to recent action taken or fines issued for non-compliance with relevant personal data protection legislation[12]. The Ghanaian DPA has recently issued fines against certain organisations in the aviation industry for breaching the Ghanaian Data Protection Act. In respect of DPAs in countries such Senegal and Tunisia, there have not been any reports of particularly robust DPA activity[13]. In contrast, the Moroccan DPA has recently investigated the data protection practices of several websites and applications which collect and process personal data in the context of providing online services[14]. In countries such as Angola, Cape Verde, Madagascar, Mali and South Africa, there has been minimal DPA enforcement and activity – for example, in South Africa, the Information Regulator (Regulator) was only recently appointed and is still in the process of getting its administrative affairs in order.

It is therefore evident that the legislative disparities as well as the disparities in DPA enforcement and activity across the African continent, pose a compliance challenge to organisations with a global as well as an African footprint.

12. Ibid 3
13. Ibid 3
14. Ibid 3

Potential Solutions for Multinational Organisations with an African Footprint to Overcome Compliance Challenges

For multinational organisations with a global and African footprint to achieve optimal compliance with disparate, or even similar personal data protection regulations, especially those in Africa, a high standard of personal data protection compliance should be applied. To use an example, the EU's GDPR or South Africa's Protection of Personal Information Act 4 of 2013 (POPI) (which is modelled on the EU's personal data protection framework, especially the Directive). If a higher compliance standard is applied, based on a particular country's legislative requirements, it would potentially streamline the compliance efforts within countries with a lower compliance standard, as there would potentially be automatic compliance due to not having to apply a lower standard of compliance. Thereafter, peculiar legislative requirements may be nuanced where necessary, and complied with once the similar legislative requirements and common personal data protection principles and themes (outlined above) have been met. Accordingly, applying a "one-size-fits-all approach" would not be prudent in ensuring that all legislative requirements have been sufficiently covered.

Considering the implementation of a globally endorsed personal data protection compliance standard: a GDPR standard

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. Organisations would still need to have a thorough understanding of the data protection legislation (if any) in the African jurisdictions in which they have a presence, and map the similarities and differences relating to the common personal data protection themes, within every pertinent piece of personal data protection legislation. This will, as part of an organisation's personal data protection programme, enable more streamlined embedding of policies, processes and procedures within business processes to achieve a level of compliance which is mature, across its entire geographical footprint. Such an approach would enable an organisation's commercial relationships to be preserved while at the same time, achieving legislative compliance. Applying the GDPR standard would also allow for disparate cross-border data transfer requirements to be more easily complied with, since the GDPR (being a high global standard) sufficiently caters for most scenarios involving the cross-border transfer of personal data and the requirements that need to be adhered to in such circumstances.

Binding Corporate Rules

In this regard, binding corporate rules (BCRs) could be utilised within a group of undertakings to ensure compliance with cross-border transfers – thereby promoting an organisation's ability to trade internationally and expand its market share and market competitiveness – irrespective of the sector or industry. BCRs are effectively intra-group personal data protection policies and procedures. They serve as a mechanism for multinational organisations with a vast African presence to share personal data within the organisation's group of undertakings, despite some of the undertakings being based in jurisdictions which do not have adequate personal data protection legislation. For cross-border data transfers to third parties outside of the multinational organisation's group of undertakings, it would be prudent to engage in a binding contract with airtight personal data protection clauses to ensure the privacy and security of any personal data shared with such third parties. Furthermore, the countries which personal data is transferred to must be assessed from a data sovereignty perspective to ensure that there are no other laws which place the personal data at risk. For example, is the government of the destination country able to subpoena such data or are there any other laws which dictate how personal data in such a country is to be dealt with?

Conclusion

Organisations with an African footprint will need to set the ball in motion as far as understanding their African personal data protection regulatory framework is concerned. Doing so would ensure that they are able to effectively capitalise on the vast investment opportunities in Africa, as personal data is the new currency with which to effectively conduct business operations globally. In this regard, all stakeholders, including an organisation's business partners, would be confident in partnering with organisations who place a high premium on personal data protection on the African continent. Hence, organisations should proactively address questions such as: "Do we know and understand our geographical footprint, especially within Africa", "do we know whether there are personal data transfer restrictions in the African jurisdictions (and elsewhere) within which we have a presence", and "are our cross-border operations legally compliant"? Our Privacy and Technology team can assist organisations in answering these questions and in effectively structuring their personal data protection compliance programmes.

Contacts

Southern Africa

Navin Sing
Managing Director: Risk Advisory Africa

Tel: +27 83 304 4225
Email: navising@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk

Tel: +27 82 415 8253
Email: dechivers@deloitte.co.za

Daniella Kafouris
Director: Risk Advisory Africa

Tel: +27 72 559 0360
Email: dkafouris@deloitte.co.za

East Africa

Julie Nyangaya
Risk Advisory Regional Leader: East Africa

Mobile: +254 720 111 888
Email: jnyangaya@deloitte.co.ke

William Oelofse
Director: Risk Advisory East Africa

Mobile: +254 20 423 0000
Email: woelofse@deloitte.com

West Africa

Anthony Olukoju
Risk Advisory Regional Leader: West Africa

Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory West Africa

Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Central Africa

Tricha Simon
Risk Advisory Regional Leader: Central Africa

Mobile: +263 772 234 932
Email: tricsimon@deloitte.com

Rodney Dean
Director: Risk Advisory Central Africa

Mobile: +263 867 700 0261
Email: rdean@deloitte.co.zw

Deloitte.

Designed and produced by Creative Services at Deloitte, Johannesburg. (000000/dbn)