

Juliet Wangui Maina Associate

jmaina@tripleoklaw.com

Tripleoklaw Advocates LLP, Nairobi

Why African countries should be concerned about the GDPR

The changes introduced by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') have been a cause for concern for many countries and businesses. It is an even bigger cause for concern in Africa, as the continent has an array of standards of national data protection legislation while many African countries have no data protection legislation at all. Juliet Wangui Maina, Associate at Tripleoklaw Advocates LLP, discusses some of the issues facing African organisations and how they can ensure compliance with the GDPR.

Although it is an EU regulation, the GDPR will undoubtedly have implications for countries in Africa. This is because, unlike the previous Data Protection Directive (95/46/EC) ('the Directive'), these GDPR will operate extra-territorially so as to apply to EU data subjects irrespective of their location. The regulations not only apply outside of the EU borders, but also carry very hefty fines for non-compliance. Failure to adhere to the provisions of the GDPR could result in fines of up to €20 million, or 4% of global annual worldwide turnover. With such fines in place, it is imperative that countries all over the world start to take steps to ensure compliance with the GDPR.

Countries in Africa have long been known for leveraging technology to leapfrog certain developmental challenges they are facing and compete in the global landscape. The ubiquity of technology has led to seamless transfers of data between organisations, countries and continents. This has presented a level of risk to all organisations leveraging technology which, if not curbed, could seriously hamper an organisations competitive advantage. Data protection regulations therefore provide safeguards which are crucial to the business life of any entity. Beyond facing this as a commercial risk, organisations now face legal risks emanating from non-compliance with the GDPR if they do process information pertaining to EU data subjects. Additionally, the GDPR also

introduces prohibition of cross-border transfers where there is no adequate data protection in the corresponding country. This essentially means that African countries that have previously been engaging with EU Member States will be restrained from doing so until they can prove compliance with the GDPR, or can demonstrate a certain level of data protection.

What is the current position in Africa?

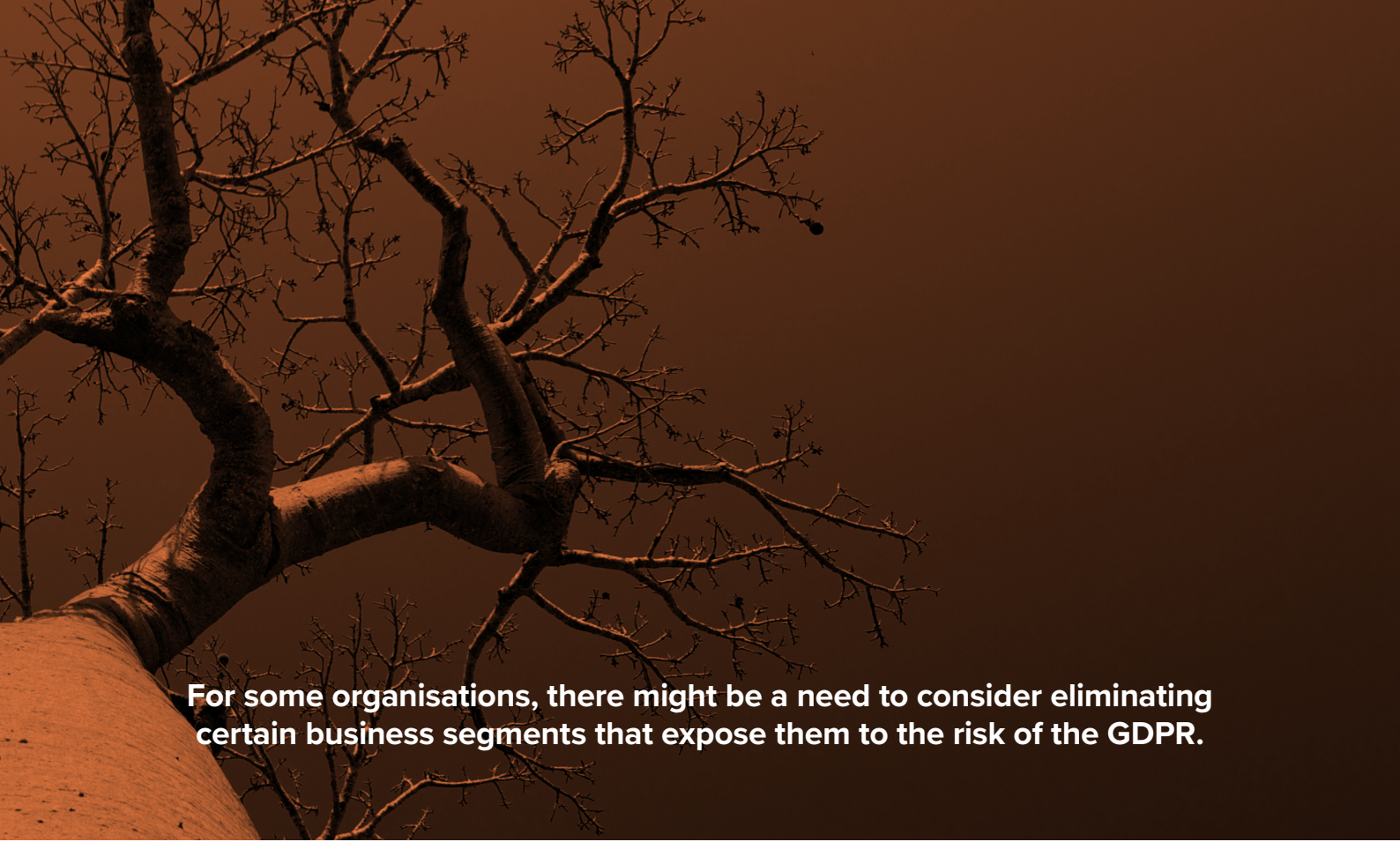
While some countries have sufficient data protection laws and authorities in place to implement these laws, others lack comprehensive GDPR compliant data protection legislation, while some have no legislation on data protection to speak of. Kenya, for example, does not have a statute specifically focused on data protection. The Data Protection Bill (2013) is based on a constitutional provision which affords every citizen the right to privacy. However, the same has not been translated into one comprehensive piece of legislation. Instead, there are certain pieces of legislation that house provisions of privacy, such as the Consumer Protection Act (2012), and others. Despite this, some of the key provisions under the GDPR do not exist in Kenyan jurisdiction, which will present a problem once the GDPR comes into force. South Africa has a Protection of Personal Information Act, 2013 ('POPI') which is similar to the GDPR in several ways, but which will still need proper implementation to ensure compliance.

Overall, most countries in Africa fall short of the requirements set out in the GDPR. Countries such as Burundi, Rwanda and Cameroon have data protection legislation in place, however, they are not at par with the GDPR and, more specifically, with the definition of personal data that has been largely expanded. At a national level, it is imperative that countries in Africa review and develop comprehensive data protection legal and regulatory frameworks to ensure that cross-border transactions with the EU are not affected. Failing this, it is expected that organisations will seek to adopt data protection policies and mechanisms at an organisational level in order to evade the hefty non-compliance fines, and to ensure that they are able to engage with businesses in the EU.

What should businesses in Africa do now?

The GDPR will be come into force on the 25 May 2018 and organisations now have just under a year to ensure they have adopted the relevant measures to ensure compliance. Beyond waiting for the national legal and regulatory frameworks to adapt to the GDPR, organisations will need to re-think their own approaches to data protection.

There are both financial and non-financial implications of ensuring compliance under this comprehensive regulation. Below are some key steps that can assist organisations on this path to compliance.



For some organisations, there might be a need to consider eliminating certain business segments that expose them to the risk of the GDPR.

Understand your organisation

The GDPR is not a one-size-fits-all regulation. This means that organisations operating in Africa will need to spend a significant amount of time analysing their organisation and their core function to understand the level of personal and sensitive data that they store. This will require a hard look at the current business, and the potential level of exposure to the GDPR non-compliance fines.

Additionally, this will also assist them in determining how much of that information is required and how they can start to comply with the data minimisation principle, by deleting all unnecessary data they may hold. For some organisations, there might be a need to consider eliminating certain business segments that expose them to the risk of the GDPR. For every organisation, it makes business sense to invest in this level of compliance.

Re-examine your data strategy

Once there is a sound understanding of the organisation's function vis-à-vis the requirements of the GDPR, it will then be necessary to re-examine your data strategy. This will inevitably vary between organisations, industries and even countries. However, the purpose of this is to provide for adequate planning and procedures that will mitigate the risk of non-compliance under the GDPR. A Privacy by Design approach will

need to be adopted when reviewing the existing strategy, to ensure that privacy is at the core of every process.

Implement policies

The GDPR builds on the Directive's principles. Therefore, this means that organisations based in the EU will already find themselves largely compliant with most of the newer provisions. However, organisations in Africa will have a harder task as some may find themselves having to implement novel policies to comply with the GDPR.

These policies will need to follow the key underlying principles of the GDPR, such as data minimisation and purpose limitations, and provide clear guidelines for what types of information will be disclosed and in what circumstances. It would be prudent for the organisation to develop a Data Protection Impact Assessment framework that would help to ensure compliance of the GDPR. The assessment would also act as a checklist which would further help in examining the vulnerabilities of the organisation in terms of implementing the GDPR.

Raise Awareness

The most crucial aspect in the process of implementing such changes in organisations is the human element. For this transition to be effective, it is paramount that all employees in an organisation understand the purpose of the GDPR and that they can act as

the front line to ensuring compliance. Therefore, the best way to effect this is through raising awareness in organisations and among employees. The privacy principles of the GDPR need to be clearly articulated to the employees to develop the culture of enhanced data protection. Ongoing workshops and training programs will act as assistance to largely mitigate the risk of non-compliance under the GDPR.

Use the GDPR to your advantage

The stringent requirements of the GDPR may seem daunting to most organisations in Africa, especially those based in countries without any data protection legislation. However, the GDPR also provides cause for organisations to re-examine their data strategies and to increase security and efficiency through better processes.

Businesses operating in Africa that can demonstrate compliance will have an added advantage as EU Member States will readily trade with them based on their compliance. Therefore, rather than considering the large task ahead that will lead to compliance, it may be more worthwhile to engage the relevant professionals and adopt organisational and technological measures that will boost your privacy landscape, while mitigating the risk of non-compliance.