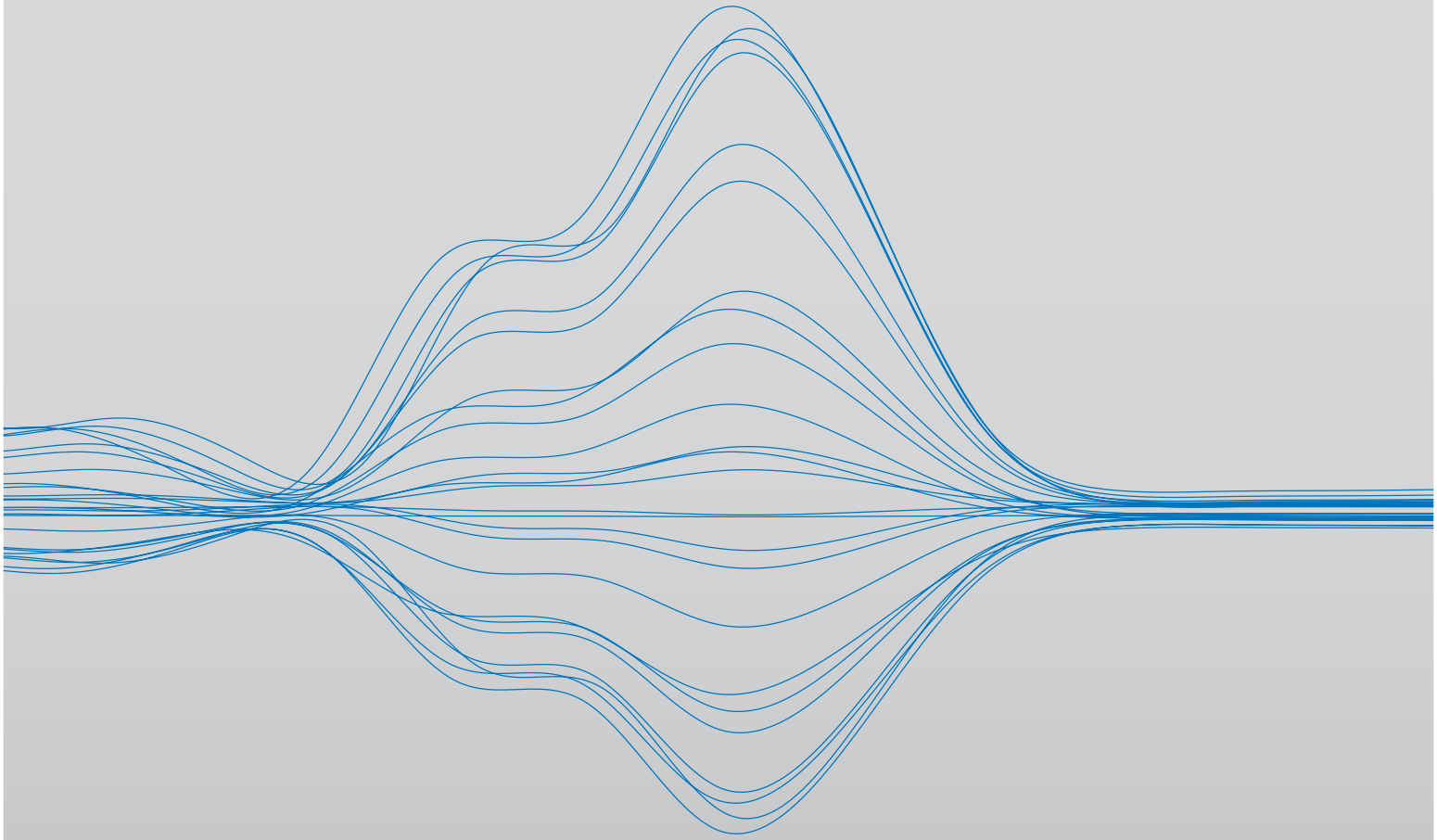
DATA PROTECTION GROUP

Practical Global Privacy



Data protection in Africa: can you take a regional approach to compliance?

DLA PIPER

AFRICA

Data protection in Africa: can you take a regional approach to compliance?

There's a wide span of maturity across the African continent when it comes to data protection legislation.

Out of 54 jurisdictions, 33 have some form of privacy regulation in place, though much of this has only come into effect during the last 10 years.

Some broad similarities between the various regimes exist. And national regulators are working together to harmonize the nuances between them, which create challenges for organizations operating across Africa – and beyond.

So what do data compliance teams need to know about the legislative landscape in Africa? What must they do to comply? And how far can they regionalize compliance across the continent?

Common ground

As many countries' regulations are based on the UN-Commission template, there are some common themes. For example, several jurisdictions in Africa require organisations to carry out the following requirements:

- *Informing data subjects of the processing* – to allow data subjects to understand what personal data is processed and why.
- *Legal basis for processing* – for a number of jurisdictions in Africa, consent of the data subject is required before processing personal data.
- *Registering with or notifying authorities* – organisations are often required to register with data protection authorities and may also be required to request prior authorization to process personal data.
- *Restricting data transfers* – common across Africa, though the provisions vary between countries. They range from the need for robust security protocols, to seeking authorization for the transfer of sensitive information.

Country-specific regulations tend to reflect differences in how recent the regulation is, and how far it has been influenced by foreign frameworks such as the European Union's GDPR. Variations can be significant, and require specific attention from data compliance teams. Breach notifications, for example, are only required in some countries.

North Africa

LEGISLATIVE OVERVIEW

Data privacy regulation varies in its sophistication across North Africa.

Morocco and Tunisia have had laws in place since around the mid-2000s. Algeria only passed data protection legislation in 2018. Egypt introduced regulation in 2020, but already had data protection provisions in place through other laws. Mauritania and Libya still have no such rules.

The more established frameworks – in Egypt, Morocco and Tunisia – are broadly similar. They follow the UN Commission template and are consent and notification-based. That means organizations must gain consent to collect or process personal data; and notify the local regulator of their intent to do so, along with the reasons why.

In Tunisia, the government had planned to reform its legislation, though this has been delayed by political instability.

Morocco is also considering an overhaul, potentially evolving its framework to more closely resemble the GDPR. As a result, the CNDP (the Moroccan data protection authority) has been encouraging organizations to carry out data-protection risk assessments.

ADVICE FOR ORGANIZATIONS

On the whole, companies operating in North Africa comply with consent rules. But meeting Morocco's' notification requirements is challenging, for two reasons:

- *Speed of processing:* It can take up to six months for the CNDP to process and issue the necessary authorizations. It's simply not practical for businesses to postpone their data processing activities for that long.
- *Lack of enforcement:* To date, the Commission has focused on educating firms on data privacy rights and protection rules. Where it has intervened, it has ordered companies to comply before considering sanctions. That said, the Commission's President has made clear that enforcement will ramp up from Q4 2022.

It therefore makes sense for businesses to submit notifications, then continue their data activities until the notification receipt or authorization comes through.

It's also worth noting that Morocco's consent exemptions are open to interpretation – in part because as the law contains no standard definition of 'legitimate interest' reasons for processing data. This can make it difficult to convince regulators that activities qualify for an exemption from the need to gain consent.

To avoiding falling into grey areas, it's better to secure consent as a matter of course, even if an exemption might apply. This is also likely to be faster than waiting for clarification from the CNDP.

West Africa

LEGISLATIVE OVERVIEW

Data protection regulation across West African jurisdictions is at different stages of development.

Cape Verde, Senegal and Ghana have had data protection laws in place for over a decade. Guinea and Nigeria's regulations only came into effect during the last six years.

Registration and processing requirements vary across the region. In Ghana, for example, businesses intending to process personal data must register with the Data Protection Commission. Those not incorporated in Ghana must register as external companies.

Senegal has no registration system. But the processing of personal data may still require prior notification to, or authorization from the national regulator.

In the region's largest economy, Nigeria, data is evolving rapidly.

Regulation came into force in 2019, followed by an implementation framework the following year. But these cover only the basic principles of data protection. And while they've helped shape compliance and enforcement, they're widely acknowledged to lack some key principles.

To rectify this, the Federal Ministry of Communications and Digital Economy called for expressions of interest from data privacy professionals to draft a new privacy law for Nigeria. In October 2022, a draft Data Protection Bill was made available to stakeholders for comment.

Among the Bill's key provisions are:

- ***Data retention***. Personal data should not be retained for longer than necessary, or beyond the period agreed with the data subjects – except with the subjects' consent.
- ***Sensitive personal data***. This can currently only be processed with explicit consent. The Bill expands the grounds for doing so to:
  - when an organization must observe data subjects' rights, or comply with obligations under employment or social security laws
  - when it's in the vital interests of the data subject, or considered substantially in the public interest, to process sensitive data

The Bill defines sensitive personal data as relating to genetics and biometrics; race or ethnic origin; religious or similar beliefs; health; sex life; political opinions or affiliations; and trade union memberships.

- ***Data breaches.*** Notifying the regulator of a breach is only necessary if there's a risk to individuals' rights or freedoms. Breaches may be announced in one or more widely used media sources, to inform data subjects who might be affected.
- ***International transfers***. Cross-border transfers are not permitted, unless necessary to adequately protect the data being processed. That protection requirement may stem from legislation: a code of conduct or certification mechanism; binding corporate rules; or contractual clauses.
- **Registration requirement**: Firms considered to be data processors or controllers of major importance must register with the NDPC. This must be done within six months of the Bill becoming law, or the company becoming a data controller or processor of major importance – which is defined as:
  - being domiciled, ordinarily resident or operating in Nigeria, and processing (or intending to process) the data of more subjects than the Commission's threshold
  - processing data that's of particular value or significance to Nigeria's economy, society or security in the view of the Commission.

Some aspects of the Bill may be revised during the legislative review process. But overall, the indications are that data protection regulation in Nigeria will move closer to the GDPR.

In addition, the government has established the Nigeria Data Protection Bureau (NDPB). This is intended to replace the National Information Technology Development Agency (NITDA) as the supervisory and regulatory authority for data protection in the country. The data protection arm of NITDA has become the NDPB, and the division of responsibilities between the two has made their roles much clearer.

Across the region more generally, we're seeing a trend towards data localization. International transfers are generally permitted, but subject to different conditions in different jurisdictions.

In Senegal, for example, the receiving country's privacy laws must offer sufficient protection for individuals' private lives, freedoms and fundamental rights. Ghana's Data Protection Act has no specific measures on transfers, but prohibits the sale, purchase or reckless disclosure of personal data.

ADVICE FOR ORGANIZATIONS

Even in countries with less robust data protection laws – or none at all – firms should comply with the highest standards of regulation they're exposed to.

Compliance should focus on areas of harmonization in the first instance, before addressing country-specific requirements. The more a programme can be built on common rules, the more efficient it will be.

From there, continuously monitoring the requirements in different jurisdictions, and how they're changing, will be essential. In some countries – Nigeria being an example – the regulators issue regular updates on data compliance matters.

The Nigerian regulator also licences data-protection compliance providers, which offer training and support to help firms follow the country's data protection rules.

East Africa

LEGISLATIVE OVERVIEW

In East Africa, even the more advanced frameworks are relatively new.

Kenya, Uganda and Rwanda have all introduced data protection laws over the past five years. Tanzania's government has recently passed the Personal Data Protection Bill 2022, which is awaiting presidential assent. Meanwhile, Burundi has no specific privacy legislation, though other laws and regulations in the country include data protection provisions.

The rules in Uganda and Rwanda require organizations that collect and process personal data to register with their respective regulators: the Uganda Personal Data Protection Officer, and Rwanda's National Cyber Security Authority.

The region's largest economy, Kenya, introduced its Data Protection Act in 2019. This requires organizations to:

- gain consent from individuals before processing their personal data
- inform them of the company's notification obligations when doing so
- retain data only for lawful purposes, and only for long enough to fulfil them
- develop, publish and regularly update a data protection policy.

Transferring data outside of Kenya is prohibited except where:

- appropriate data protection safeguards are in place in the receiving country
- the Data Protection Commissioner has made an adequacy decision relating to the receiving country
- the data subjects have given their consent
- the transfer is necessary in order to:
  - carry out contractual obligations
  - protect the public interest
  - protect the interest of individuals who can't physically or legally give consent
  - protect the interests of the organisation, where these aren't overridden by those of the data subjects
  - bring or defend a legal claim.

Meanwhile, some of the Act's requirements apply only in certain cases:

- Firms with annual revenues of at least KES5 Million (c.USD50,000), and ten or more employees, must register as a data controller and/or processor with the Office of the Data Protection Commissioner (ODPC).
- Businesses must conduct a Data Protection Impact Assessment if their processing activities present a high risk to the rights of data subjects.
- A Data Protection Officer must be appointed in some circumstances, such as when processing sensitive data.

Not complying with the Act can lead to fines of up to KES5Million, or 1% of turnover for the previous financial year (whichever is lower).

ADVICE FOR ORGANIZATIONS

Wherever they operate in East Africa, firms must ensure they fully understand the regulation in the relevant jurisdictions, and how it differs between countries.

International organizations may also need to identify where local requirements vary from those in the European GDPR.

When processing data in Kenya, Rwanda and Uganda in particular, we'd advise businesses to:

- develop or update data protection policies and procedures in line with local requirements
- make sure they understand the restrictions on data transfers, and how to comply with them
- register with the ODPC in Kenya, and any other countries' authorities as necessary.

Southern Africa

LEGISLATIVE OVERVIEW

Most Southern African countries have data protection legislation frameworks in place.

Broadly speaking, these are similar to the GDPR, and cover data-subject rights, cross-border transfers, and how to respond to data breaches. Most provide data subjects with grounds for refusal, and countries with a regulator require companies to register with it.

However, the extent of protection provided varies between countries.

The more established regimes are found in Angola, Mauritius, South Africa and Zambia.

Zambia, for example, introduced the Data Protection Act No. 3 of 2021. This sets out comprehensive regulations for the collection, use, storage and disclosure of personal data, along with stringent rules on cross-border transfers. It also requires firms to register with the data regulator, and governs the licensing of data auditors.

Mozambique and Namibia have no comprehensive data protection legislation, though sector-specific and other privacy-related laws do protect client information.
In Zimbabwe, the landscape is evolving. The country's primary source of data legislation is the Cyber and Data Protection Act (Chapter 12:07), enacted in 2021.

Botswana now has a Data Protection Act (DPA) in place, and a newly established Information and Data Protection Commission. Compliance with the DPA has only recently become necessary (as of September 2023).

Thanks to the Protection Personal Information Act (POPIA), South Africa's rules are more onerous than elsewhere in Southern Africa:

- The POPIA applies not just to natural persons, but also to the personal information of juristic persons (e.g. the contact details and financial information of companies). Most countries' data privacy laws – including the GDPR – only cover individuals.
- The threshold for communicating breaches is lower than in most countries. The Information Regulator (IR) and affected data subjects must be notified of a breach as soon as reasonably possible – if there's reasonable suspicion that personal information has been accessed or acquired by an unauthorized party.
- Firms need approval from the IR before carrying out some processing activities. For example, transferring sensitive personal information or children's data to third parties in countries where data protection is deemed inadequate.

Until now, regulators in Southern Africa haven't been particularly active on the enforcement front: no publicized penalties have been issued in the region. However, that's likely to change – especially in South Africa, where the IR is upping its capacity.

ADVICE FOR ORGANIZATIONS

International organizations should follow a number of important steps to ensure compliance in Southern Africa:

- Register with the local data regulator in each country where they operate.
- Adapt data collection and processing procedures to local nuances in those countries – especially the 'outlier' POPIA provisions in South Africa.
- Implement procedures for data subjects to exercise their rights under local laws – the right of refusal in particular.
- Make sure internal controls and procedures comply with the rules on cross-border data transfers.
- Put robust data-transfer agreements in place – including adequate remedies – with suppliers abroad that handle data on their behalf.
- Ensure a robust response to any breach in countries with little or no data regulation.

Build compliance from the regional minimum

Data protection laws, and the cultural backgrounds that inform them, vary between jurisdictions in Africa. Similarly, the levels of maturity, severity and complexity of regulations may differ from one country to the next. That's true even where countries' regulations are based on the UN-Commission template.

As such, the commonalities highlighted above amount to the minimum level of data protection required when operating across the continent. Beyond that, global compliance teams must work with local counsel to identify specific requirements in each country, and adapt their privacy policies accordingly.

As they do so, they should keep the following recommendations in mind:

- Don't assume regulations based on GDPR will operate locally in the same way as in Europe.
- Get to know local regulators' attitudes and approaches to enforcement. That will enable you take a risk-based approach to compliance – which will in turn help optimize your resource allocation.
- Make sure you understand the cultural perceptions and relationships relating to data in each market. Knowing them will drive opportunities to enhance customer engagement and exploit commercial opportunities.

In addition, businesses should work on the basis that they will suffer a data breach at some point – and prepare thoroughly for one.

That should involve:

- ensuring everyone knows their role in responding: IT, compliance, communication and legal (including external partners)
- rehearsing the response procedure periodically
- rolling out regular education, training and awareness-raising – to all staff, at all levels, throughout the employee lifecycle.

Ultimately, it's vital to remember the reputational damage a breach can have – locally and globally. Strong data protection safeguards are always advisable, even where enforcement action may be unlikely.

Carolyn Bigg
Partner
T +852 2103 0576
carolyn.bigg@dlapiper.com

Livia Dyer
Partner
T +27 (0) 302 0849
livia.dyer@dlapiper.com

Monique Jefferson
Partner
T +27 (0)11 302 0853
monique.jefferson@dlapiper.com

William Maema
Senior Partner
T +254 20 277 3000
william.maema@ikm.dlapiperafrica.com

Adewumi Salami
Senior Associate
T +234 1 279 3670
adewumi.salami@oo.dlapiperafrica.com

Adil Mouline
Associate
T +212 520 427 854
adil.mouline@dlapiper.com