University of New South Wales Law Research Series

NIGERIA REGULATES DATA PRIVACY: AFRICAN AND GLOBAL SIGNIFICANCE

GRAHAM GREENLEAF

(2019) *158 Privacy Laws & Business International Report* 23
[2019] *UNSWLRS* 66

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Nigeria regulates data privacy: African and global significance

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia*
(2019) 158 *Privacy Laws & Business International Report*, 23-25

The regulation of data privacy by Nigeria, the most populous country in Africa and the seventh largest in the world (186 million), is an event of significance in the evolution of the world's data privacy laws. Other factors also make Nigeria significant for privacy: it has Africa's largest economy, overtaking South Africa in 2014; as an officially English-speaking country, it will help open up a broader discussion of data protection in a continent dominated by francophone progress (South Africa's developments having been moribund as yet); and as a country with roughly equal Muslim and Christian populations, it joins Indonesia, Turkey and Malaysia as major Muslim countries with data privacy laws.

The Nigerian Information Technology Development Agency (NITDA) issued the *Nigerian Data Protection Regulation 2019* ('the Regulation')[1] on 25 January 2019, coming into effect immediately upon issue (Preamble). The Regulation is made pursuant to the *Nigerian Information Technology Development Agency Act of 2007* (*NITDA Act)*. Although the Act makes it a function of NITDA to 'develop guidelines for electronic governance' (and so on) (art. 6(c)), and to 'make such regulations as in its opinion are necessary or expedient for giving full effect to the provisions of the Act' (art. 32), it does not say, unlike the Preamble to the Regulation that the Act authorizes it to 'develop regulations for electronic governance'. There is therefore perhaps some doubt as to whether the Regulation is *ultra vires*, but this article proceeds on the assumption that it is valid.

Previous Guidelines on Data Protection 2013, issued by NITDA, did not qualify as a data protection law, both because of deficiencies of content, and lack of enforceability. The Regulation of 2019 does not share these deficiencies. The Regulation may eventually be replaced by a stand-alone primary law. The *Digital Rights and Freedom Bill*, which passed both houses of the Nigerian Parliament in 2018, has in March 2019 been refused signature by newly re-elected President Buhari, on the grounds that it covered too many subject-matters in too little detail, and overlapping other pending Bills.[2] At least for now, this Regulation under the NITDA Act is Nigeria's first data privacy law, and is very detailed on data protection compared with that Bill. This article will identify the main features of the Regulation, emphasising its similarities to and differences from the European Union's *General Data Protection Regulation* (GDPR).

Nigeria's regional obligations

Nigeria is the 26th African country to regulate data privacy (of 54 African Union member states), and the 134th in the world. It is not yet a signatory to the African Union's data protection Convention.[3] However, as a party to the treaty establishing the Economic

* *Bertil Cottier provided valuable information for this article, but responsibility for all content remains with the author.*

[1] *Nigerian Data Protection Regulation 2019*

[2] 'Buhari declines assent to Digital Rights and Freedom Bill, four others' The Guardian (Nigeria) 20 March 2019 <https://guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/>

[3] *African Union Convention on Cyber-security and Personal Data Protection*, open for signature in 2014.

Community of West African States (ECOWAS), it is bound by the *Supplementary Act on Personal Data Protection Within ECOWAS* (2010), the only binding data protection agreement in force in Africa. The Regulation may make Nigeria the 10th of fifteen ECOWAS states to comply with that obligation, though issues arise concerning full compliance (discussed below).

Scope of Regulation

The scope of the Regulation is the same as for the GDPR on most important issues: the definitions of 'data subject'; 'personal data' (both in terms of 'identifiability'); 'data controller' (and 'data administrator' to mean the same as 'data processor') are all familiar from the GDPR. 'Sensitive personal data' includes 'any other sensitive personal information', and so is probably broad enough to include biometric and genetic information.

The Regulation 'applies to all transactions intended for the processing of Personal Data,' (cl. 1.2(a)), and thus to the whole of the private and public sectors, as confirmed in the Preamble. Such transactions are stated to be 'in respect of natural persons in Nigeria'. The Regulation also applies to persons 'residing outside Nigeria who are citizens of Nigeria' (cl. 1.2(b)), but this might be read to apply only when the processing concerned takes place in Nigeria. Unlike the GDPR, there is no application to extra-territorial processing targeting Nigerian residents.

The Regulation also has no application to processing concerning foreign non-residents of Nigeria, even if it takes place within Nigeria. Nigeria's law will therefore not apply at all to personal data transferred to Nigeria from overseas, including from the EU. This 'outsourcing exemption' should be a fatal defect in relation to EU adequacy, which is odd for a law which is otherwise clearly intended to emulate many aspects of the GDPR, and means that transfers from the EU to Nigeria for outsourced processing will need to have other 'appropriate safeguards' or applicable exceptions.

Enforcement and administration

The Regulation designates the NITDA as 'the Agency' to administer the Regulation (cl. 1.3(xxvi)), and gives it various powers, for example to licence Data Protection Compliance Organisations, to receive audit information, to make adequacy decisions in relation to foreign countries, and to develop and manage international cooperation mechanisms (art. 4.3). It therefore appears that NITDA is the data protection authority (DPA) for Nigeria.

NITDA is not independent, because the Minister may give it general directions concerning the carrying out of its functions (NITDA Act 2007, art. 27). This is not consistent with the ECOWAS Supplementary Act requirement of an independent DPA.

In relation to civil remedies such as compensation, NITDA is to establish an Administrative Redress Panel to investigate allegations of breach of the Regulation, issue administrative orders pending the outcome of investigations, and determination of appropriate redress, with breaches of the Regulation being construed as breaches of the NITDA Act (cl. 4.2). Individuals also retain their right to 'seek redress in a court of competent jurisdiction' (cl. 4.2(1)). It is not clear from the *NITDA Act* that breaches of the NITDA Act could result in such redress.

Data controllers (but not data administrators/processors) are also liable for fines for breaches ('in additional to any other criminal liability'). If they deal with more than 10,000 data subjects annually, the fine is 2% of 'annual gross revenue' (presumably domestic, not global), or 10M Nigerian Niara (about US$27,500), whichever is greater. For controllers dealing with fewer than 10,000 data subjects annually, the fine is 1% or US$5,500. Unless very robust assessments of annual gross revenue are made, these fines are unlikely to be major deterrents.

The Regulation establishes a compliance oversight system under NITDA control (cl. 4.1):

- All controllers must publish, within three months, data protection policies complying with the Regulation;
- Each controller must designate a Data Protection Officer (DPO) to ensure compliance, but the data controller may 'outsource data protection to a verifiably competent firm or person';
- All controllers must conduct 'a detailed audit of its privacy and data protection practices' (with minimum details specified) within six months, and provide a summary to NITDA, and annually thereafter (depending on number of data subjects);
- NITDA will register, licence and regulate Data Protection Compliance Organisations (DPCOs) who shall, 'on behalf of' NITDA', monitor, audit, and train all controllers, as well as advise on compliance.

It is not clear whether a DPCO can also be an outsourced DPO, and whether licensed DPCOs have a monopoly on compiling and submitting audits. There is considerable potential for conflicts of interests in these arrangements. Both the AU Convention and the ECOWAS Supplementary Act envisage some formalities of at least DPA notification of processing. This may be the reason why the Regulation does so even though the GDPR does not, although the above requirements could also be seen as consistent with an extensive version of the GDPR's Data Protection Impact Assessment (DPIA) requirements.

Controller obligations

The requirement of 'lawful processing' is central, as with the GDPR, but the ground of processing to protect the legitimate interests of a controller is absent (cl. 2.2). Other fundamental obligations include data quality, storage limitation and security, the existence of a duty of care on anyone entrusted with personal data, and accountability for compliance with 'the principles contained' in the Regulation (cl. 2.1). These give a basis for enforcement.

Almost all aspects of the GDPR's stronger approach to consent are present, either in the definition of 'consent', or the detailed restrictions on obtaining it (cl. 2.3). A strong element is the high level of obligations and liability that data controllers have for the data 'administrators' (processors) that they choose, including a due-diligence-like obligation to check their record in previous handling of personal data (cl. 2.4). Written contracts requiring adherence to the Regulation are required (cl. 2.7).

Data subject rights

Many GDPR-like data subject rights are provided, including (cl. 3.1) notice of:

- Transparency when providing access to data subjects;
- Detailed notice prior to collection of personal data (cl. 3.1(7)), including
    - Existence of automated data processing, with 'meaningful information about the logic involved';
    - Intent of processing for purposes other than that for which the data are collected (side-stepping the otherwise apparently strict limits in cl. 2.1(1)(a));
    - Whether an intended transfer to a foreign country is to one where the NITDA has made an adequacy decision (but only the right to be informed of any safeguards to be adopted, not automatic notice);
- Correction and supplementation, with advice to previous recipients (cl. 3.1(8), (13));
- Deletion / 'right to be forgotten' in similar terms to the GDPR (cl. 3.1(9)-(10), (13);
- Restrictions on processing, also in similar terms to the GDPR (cl. 3.1(11)-(12));
- Data portability (cl. 3.1(14)-(15)).

Other provisions also create rights for data subjects, including to opt-out of processing for marketing and other purposes (cl. 2.8).

Data transfers

The NITDA decides whether a foreign country 'ensures an adequate level of protection', but this is subject to the 'supervision' of the Attorney-General, who is to take into consideration much the same factors as are stated in GDPR art. 45 (cl. 2.11). It is also implied that the Attorney-General can make such decisions independently of NITDA. If no positive decision concerning adequacy has been made, exceptions allow transfers on various grounds (cl. 2.12), similar to GDPR art. 49 derogations. There are no 'appropriate safeguards' as alternatives (BCRs etc).

Conclusions

This law has more common features with the GDPR than most of the other 23 data privacy laws in Africa. However, it has many significant limitations. Its validity is questionable. A major deficiency is that it does not provide any protection to foreign-sourced data processed in Nigeria. Its enforcement measures might not be a significant deterrent to breaches of its principles. Its provisions for Compliance Organisations could result in conflicts of interest. This Regulation may not be Nigeria's final data privacy law, but it is a notable step in that direction, and because of the importance of Nigeria, a significant step for Africa.