The African Union's data privacy Convention: A major step toward global consistency?

Graham Greenleaf and Marie Georges*

(2014) 131 *Privacy Laws & Business International Report,* 18-21.

At various times over the past 40 years, differing regions of the world have become the most active 'growth areas' in the global diffusion of data privacy laws, now found in 105 countries. This was so for Western Europe in the 1970s and 1980s, Latin America in the 1990s (with the constitutional 'habeas data'), Eastern Europe in the 2000s, and Asia in 2010-13.[1] Now it is Africa that is leading global expansion, with 15 countries having enacted laws. African countries have consistently developed data privacy laws for over a decade, in Cape Verde (Cabo Verde, 2001, amended 2013), Seychelles (2003), Burkina Faso (2004), Mauritius (2004), Tunisia (2004), Senegal (2008), Benin (2009), Morocco (2009), Angola (2011), Gabon (2011), Ghana (2012), Lesotho (2012), Ivory Coast (Cote d'Ivoire, 2013), Mali (2013), and in the key economy of South Africa (2013). There are also many Bills in progress, sub-regional instruments, a civil society Declaration and finally a new African Union Convention on cyber-security and data protection that potentially spans the whole continent. This article gives an overview of the new Convention and other pan-African developments. In future issues we will consider sub-regional developments and survey the twelve African countries with data privacy laws, particularly the four new laws of the past year.

African Union data protection Convention 2014

The potentially most important development in Africa is the adoption on 27 June 2014 of the *African Union Convention on Cyber-security and Personal Data Protection*,[2] at the African Union's Summit in Malabo, Equatorial Guinea. The African Union (AU), which has as its members all 54 African states except Morocco, was developing since at least 2011 a draft Cyber-security Convention (now re-named to include data protection). Inclusion of Chapter II of the Convention, 'Personal Data Protection', means that State parties who accede to and ratify the Convention are committed to 'establishing a legal framework' based on its provisions, although this is stated to be 'without prejudice to the free flow of personal data' (Art. 8). Africa is now the first region (in fact a continent) outside Europe to adopt a data protection Convention as a matter of international law, but it will require accession by fifteen states before it is in force.[3]

---

* Authors: Graham Greenleaf is Professor of Law & Information Technology at UNSW Australia, and PL&B's Asia Pacific Editor. Marie Georges has been an activist for a world instrument in data protection since the early 1970s, is a former counselor to CNIL's chairman, and a founder of the francophone association of DPAs, and as a Council of Europe expert she is currently involved in a EU/CoE cooperation project in Ukraine.

[1] Graham Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2014) *Journal of Law, Information & Science* <http://ssrn.com/abstract=2280877>.

[2] African Union Convention on Cyber-security and Personal Data Protection (27 July 2014) < http://opennetafrica.org/wp-content/uploads/researchandpubs/African%20Union%20Convention%20on%20CyberSecurity%20&%20Personal%20Data%20Protection.pdf>

[3] The AU Convention has more potential state parties than any other international data protection agreement currently has ratifications. Council of Europe Convention 108 has 46 ratifications, and one accession not followed by ratification, but is open to non-European states (Greenleaf: 'Uruguay starts Convention 108's global journey with accession'). Fifteen ratifications are required for the AU Convention to enter into force (Art. 36). A Status List for this Convention has not yet been published by the AU (http://www.au.int/en/treaties), and no accessions or ratifications within its first three months are known. The Chairperson of the AU Commission is to submit reports to the Executive Council of the AU progress made by each State Party to the Convention on implementation of its provisions.

Scope of the Convention

The starting points are conventional EU-influenced definitions of 'personal data' in terms of direct or indirect identifiability of a person, of 'processing' in broad terms, and of a 'data controller' (Art. 1). Its scope (Art. 9) extends to the public and private sectors generally, and to automated and non-automated processing. Processing relating to 'public security, defence, research, criminal prosecution or State security' is covered but allowed to be subject to some exceptions defined by specific provisions in existing laws. Processing exclusively for an individual's 'personal or household activities' is exempt, but not where 'for systematic communication to third parties or for dissemination'. Any processing for journalistic or research purposes is exempt, if conducted within professional codes of conduct, as well as any processing for artistic or literary expression (Art. 14.3).

The privacy principles in the Convention

Articles 13 to article 23 set out the substantive principles with which data controllers must comply, and the rights of data subjects, in ways which are very consistent with 'European' approach (the Council of Europe approach, as developed by the EU). The 'Basic Principles' (Art. 13) include that legitimacy of processing is based on consent (with specified exceptions); lawful and fair processing; processing for specific purposes, and those compatible with them; collection limited to data 'adequate, relevant and not excessive' for those purposes', and generally retained for no longer than necessary for them; with reasonable steps to keep them accurate and up-to-date; processed transparently; and kept with security and confidentiality by controllers and processors.

There is a prohibition on any processing of 'sensitive data', unless one of ten exceptions is satisfied (Art. 14). This applies to data 'revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject' (Art. 14), a description differing from the definition of 'sensitive data' (Art. 1), which also includes 'social measures', 'legal proceedings and penal or administrative sanctions' (none of which are protected by Art. 14). 'Biometrics' are not included in either definition (while it is included in the SADC model law), and so are not protected against over-collection. 'Parental filiation' is an unusual inclusion, but is of particular significance in some sub-Saharan countries due to beliefs that knowledge of the identity of a person's biological parents can be used in spells to harm them.

As in the EU, decisions which substantially affect a person are not allowed to be based solely on automated processing intended to evaluate aspects of the person's prospective behavior, based on profiling data (Art. 14.5). 'Interconnection of files' (or 'data matching') has to meet substantive goals and not leading to discrimination (Art. 15), but also obtain authorization (see below). The data subject's rights include notification, access, objection to processing (including notification and opt-out rights in relation to marketing uses), rectification and blocking (Arts. 16-19). Data controllers have obligations of confidentiality, security, retention limitation and 'substainability' of utilisation despite technological changes (Arts. 20-23).

Complexities with direct marketing

Situated in the Electronic Transactions chapter (and therefore outside the Data Protection chapter) are requirements that direct marketing by 'indirect' communications (defined as allowing storage until accessed – e.g. email, voicemail) can only be carried out with prior consent, except for some email marketing of similar products, where the data subject's contacts have been obtained from him or her. Contact particulars to facilitate opting out at no charge must always be provided (Art. 6). There is little coordination between these provisions and those giving a more general rights to object to processing (Art. 18(2)).

Enforcement structure and processing formalities

An independent national data protection authority (DPA) is required by the Convention, comprised of members independent of government or the information and communications sectors, with immunity from suit and who shall not receive instructions from other authorities (Art. 11). The DPA must have broad powers, including (subject to appeals in all cases) to investigate, give opinions, give warnings, inform judicial authorities of offences, impose monetary fines, give and withdraw authorisations of various types, and discontinue or block processing where fundamental rights are threatened (Art. 12). The details of such enforcement measures are generally left to State parties. However, where computer systems are used to disclose some of the categories of sensitive data, for the purpose of threatening offences against, or insulting, persons in those categories, harsh criminal penalties are required (Art. 29.3 (f) and (g)).

Most processing is required to be subject to formalities, of three types:

(i) Prior 'authorization' by the DPA is required for processing of various types of sensitive data or of ID numbers or similar, or interconnection of files (Art. 10.4);
(ii) 'Informed advice' by the DPA, for various types of processing by bodies with public obligations (Art. 10.5); or
(iii) 'Declaration' to the DPA (Art. 10.2)

Details are specified as to what particulars must be provided to the DPA (Art. 10.6). Processing is exempt from formalities where the DPA has exempted or simplified declaration procedures because it is 'not likely to constitute a breach of privacy or individual freedoms', or it is (in essence) for purely internal use of an organisation or private use of a person (Art. 10.1-3). The cybercrime provisions require criminal offences where a controller or processor undertakes processing without observing the necessary formalities 'even through negligence' (Art. 29.2(e)).

Data export and extraterritoriality provisions

Data controllers 'shall not transfer personal data' to States outside the AU unless the State of the recipient 'ensures an adequate level of protection' (Art. 14.6(a)). Although 'adequacy' is not defined, the implication is that it has a meaning informed by the usage of the same term by Article 25 of the European Union's data protection Directive. It is not explicit how findings of 'adequacy' are to be made. One could have thought however to phrase it in a more understandable legal language along with a "legal framework with a similar effect" .

The 'adequacy' provision does not, however, apply where 'the data controller shall request authorization' from the DPA (Art. 14.6(b)). Such 'authorization' of processing (which includes exporting[4]) is required for some categories of sensitive data (Art. 10.4). However, the DPA is also given the specific power of 'authorizing trans-border transfer of person data' (Art. 12.2(k)). Although it is not explicit, this may envisage that the DPA can authorize transfers of personal data based on pragmatic legal tools,[5] binding corporate rules (BCRs) or Common Contract Clauses (CCCs) as an alternative to the 'adequacy' approach.

The 'adequacy' requirement does not apply to other AU member states, whether or not they have ratified the Convention. This could mean that Convention parties can adopt any export provisions they like in relation to other AU members, ranging from no export restrictions, to

[4] Processing includes 'disclosure by transmission, dissemination or otherwise making available' (Art. 1 definition).

[5] They were originally developed in the early 80s by the French DPA and subsequently developed by the Council of Europe, European Commission and the article 29 Working party.

the same 'adequacy' rule as for other States (a more restrictive standard is unlikely). However, it may also be interpreted to imply that data exports to other AU member states will require authorization by the DPA under Art. 12. Unlike Europe's Convention 108, or the EU's Directive, it does not require 'free flow' of personal data between parties to the Convention, a deficiency in inducements which may slow down accessions and ratifications.

The Convention only applies to 'processing of data undertaken in the territory' of an AU state (Art. 9.1(c)), so extra-territorial application is not required, but nor is it forbidden. In relation to both these aspects of the international movement of personal data, the Convention is therefore consistent in only requiring minimum standards of protection, but allowing more extensive protections.

Nature and role of the AU Convention

From the above summary, it can be seen that the Convention's principles, and its enforcement and other procedures, are clearly more influenced by European approaches than those of the OECD. They require laws that are quite prescriptive, and with a moderately high level of administrative requirements considered as a DP awareness, communication and control tool. The level of detail of the data protection aspects of the Convention are such that an African country could extract them as the basis for national legislation, requiring only a modest amount of detail to be added. While the Convention provisions are almost a 'model Act', the extent to which they are consistent with sub-regional developments in Africa, particularly the ECOWAS Supplementary Act and the use of the SADC 'Data Protection Model Law' (discussed in a following article) need consideration.

Civil society's Africa-wide Internet Declaration

Only a few weeks after the AU Convention adoption, 21 civil society organisations working on Internet governance in Africa, including many of the most prominent human rights organisations in Africa, also launched an *African Declaration on Internet Rights and Freedoms*.[6] Two of the Declaration's twelve 'Key Principles' are demands for protections on the Internet of privacy (including personal data), and data security.[7] The Declaration also includes strong statements against mass surveillance.[8]

The elaboration in the Declaration of what is required to realise these principles calls for 'compliance with well-established data protection principles', which in the African context perhaps should be taken as referring to the principles in Chapter II of the AU Convention, although it is not mentioned.

---

[6] African Declaration on Internet Rights and Freedoms <http://africaninternetrights.org/> , launched at the 18th annual Highway Africa Conference at Rhodes University in Grahamstown, South Africa on 7 September 2014, following a soft launch a week earlier at the Global Internet Governance Forum in Istanbul: see <http://www.article19.org/resources.php/resource/37682/en/african-declaration-on-internet-rights-and-freedoms-launched>.

[7] '**Privacy:** Everyone has the right to privacy online including the right to control how their personal data is collected, used, disclosed, retained and disposed of. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards. **Security on the Internet:** Everyone has the right to security on the Internet and to be protected from harassment, stalking, people trafficking, identity theft and misuse of one's digital identity and data.'

[8] 'Mass or indiscriminate surveillance of the people and the monitoring of their communications constitutes a disproportionate interference, and thus a violation, of the right to privacy. Mass surveillance should be prohibited by law. The collection, interception and retention of communications data amounts to an interference with the right to privacy whether or not those data are subsequently examined or used.'

Among the bodies which the Declaration calls on to implement it, are the African Commission on Human and Peoples' Rights (to monitor Internet rights and freedoms in Africa), and UNESCO (to draw up model laws protecting online privacy). The African Charter on Human and Peoples' Rights (1981)[9] makes no reference to privacy (unlike other equivalent regional instruments or the International Covenant on Civil and Political Rights), and it will be interesting to see if the Convention influences changes to that aspect of the Charter. The Declaration will be presented at the African Union Conference of Ministers in charge of Communication and Information Technologies in early 2015.[10] The call for data privacy protection in Africa is therefore now coming from both government and civil society alike, though with different emphases.

Conclusions – International standards and growth factors in Africa

It has taken Europe over 30 years since 1981 to do so, but 45 of 47 Member States of the Council of Europe have now ratified Convention 108 and enacted data privacy laws as well. The equivalent developments in Africa cannot be expected to happen overnight, but a comparable continentally comprehensive and relatively uniform adoption of data privacy laws may well result in Africa. The global consequences for the irreversibility of data privacy laws, and their consistency based around a European-influenced model, are very significant.

The most important indicator whether such a development is likely is how quickly African countries with data privacy laws, particularly countries with major economic and political weight like South Africa, will accede to and ratify the Convention. Second is the extent to which countries which do not yet have such laws start to enact Convention-compatible laws.

As will be discussed in later articles in this series, there is considerable interest in African countries in being recognised as adhering to increasingly universal data privacy principles as developed in their 'European' form. Many are likely to be interested in recognition of 'adequacy' by the EU, or in adhering to Council of Europe Convention 108,[11] or both. In comparison, no African countries are known to have declared that they adhere to the OECD privacy Guidelines, which is now possible after the 2013 revisions to the Guidelines.[12]

There is as yet no organisation linking only the DPAs in African countries, unlike in most other regions.[13] The Convention makes it a goal of African DPAs to set up such cooperation mechanism among themselves and with other DPAs (Art. 12. 2(m)). Moreover, it is possible that such a development might be prompted along with the first African DPA hosting of the annual International Conference of Data Protection and Privacy Commissioners (ICDPPC), in Mauritius in 2014. As mentioned, AFAPDP is already a meeting point for some.

---

[9] African Charter on Human and Peoples' Rights (1981) <http://www.achpr.org/instruments/achpr/>.

[10] 'About' page of the Declaration < http://africaninternetrights.org/about/>.

[11] While Morocco is not in AU, it is the first African country to have been invited to accede to Convention 108 (on 30 January 2013), accession still pending but expected to be finalised early 2015. Other announcements of requests to accede are also expected soon.

[12] Graham Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014) <http://ukcatalogue.oup.com/product/9780199679669.do>, Chapter 19.

[13] Greenleaf 'Sheherezade and the 101 data privacy laws'

Finally, there is the question of how the African Union itself is likely to be integrated into a global privacy agreement. The UN does not seem likely to move toward any binding treaty, so the AU will need to consider joining agreements such the Council of Europe Convention 108, which will become open to regional and other organizations (as it is currently open to third countries) according to the current 'modernisation' draft to reform the Convention. It is likely that the monitoring mechanism to be set up for the AU Convention (Art. 32) would support this.

This is a slightly expanded version of the article published in (2014) 131 Privacy Laws & Business International Report, 18-21, adding the list of all African countries with privacy laws.