

African regional privacy instruments: Their effects on harmonization

Graham Greenleaf and Marie Georges.

(2014) 132 *Privacy Laws and Business International Report* 19-21, December 2014

Contents

The ECOWAS treaty commitments	2
The HIPSSA model laws – the ITU and EC support for harmonisation	2
Southern Africa (SADC)	3
East Africa (EAC)	3
Central Africa (ECCAS /CEMAC)	4
North Africa	4
Content of the agreements and model laws.....	4
Conclusions: The international context of African harmonisation.....	5

African countries started to adopt data protection laws because of mainly national preoccupations related to the growing use of computers to manage State activities such as issuing identification documents (Burkina Faso 2004) or electoral lists (Benin 2009), and because of the growing operation of private outsourcing activities from European countries (Mauritius and Tunisia 2004; Senegal 2008; Morocco 2009). Despite these disparate and complementary origins, there are now strong moves within sub-regions of Africa promoting harmonisation of data protection laws, as well as at the regional level Africa as a whole (the recent continent-wide African Union Convention and the civil society Declaration – see Greenleaf and Georges, PL&B International, Oct 2014).

This article focuses on the sub-regional developments. Africa's 54 countries have important data privacy agreements and model laws in sub-regions or Regional Economic Communities (RECs) of Africa.¹ Africa has at least eight RECs,² but only four are as yet significant in the data privacy context: ECOWAS (west); SADC (south), ECCAS and CEMAC (central) and EAC (east). The scope and purpose of these sub-regional developments is now outlined, focusing on their influences and history.

¹ See 'African Union (AU) & Regional Economic Communities (RECs) In Africa' UN Economic Commission for Africa <<http://www.uneca.org/oria/pages/african-union-au-regional-economic-communities-recs-africa>>.

² CEN-SAD; COMESA; EAC; ECCAS; ECOWAS; IGAD; SADC; and UMA. See links in footnote 1 for details.

The ECOWAS treaty commitments

The strongest developments as yet, and the earliest, have been from the Economic Community of West African States (ECOWAS), a grouping of fifteen states³ where French, Portuguese and English are variously spoken. Under the Revised Treaty of the ECOWAS they agreed in 2008 to adopt data privacy laws. A *Supplementary Act on Personal Data Protection within ECOWAS* (2010) to the ECOWAS Treaty, adopted by the ECOWAS member states, establishes the content required of a data privacy law in each ECOWAS member state, including the composition of a data protection authority. This is the only binding regional/international data protection agreement yet in force in Africa. In addition, once this framework is completed, it may be enforced by the ECOWAS Court of Justice. All requirements are influenced very strongly by the EU data protection Directive as developed in the DP law of Senegal. Seven ECOWAS states have enacted laws (Benin, Burkina Faso, Cape Verde, Senegal, Ghana, Ivory Coast and Mali), and Bills are under elaboration or consideration in Nigeria, and Niger, leaving only six yet to take any action. In some of the ECOWAS member states without separate legislation as yet, the ECOWAS Supplementary Act, as an additional protocol to a treaty, may be legally binding in creating substantive rights in countries where treaties have direct effect and do not require local enactment. This appears to be the case in Niger, where a law is being developed to establish a DPA, to complement the ECOWAS treaty on data protection, which was published in Niger's official journal in 2013. The ECOWAS Supplementary Act was a project assisted by the EU/ITU in 2005-7, as a precursor to the broader HIPSSA initiative.

The HIPSSA model laws – the ITU and EC support for harmonisation

In parallel with the ECOWAS developments, the International Telecommunication Union (ITU), with financial support from the European Union (EU), developed from 2008 onward a project with African countries on a subregional basis called HIPSSA (*Harmonization of ICT Policies in Sub-Sahara Africa*).⁴ The project is aimed at harmonisation (or initial adoption) of the numerous telecom laws needed for liberalisation of telecoms competition and a telecoms regulatory framework, with data protection and cybercrime laws as part of the overall HIPSSA package. Built upon the ECOWAS ITU/EC pilot, the HIPSSA Project was initiated as a result of the request made by the economic integration organizations in Africa, as well as regional regulators' associations, to the ITU and EU for assistance in harmonizing ICT policies and legislations in sub-Saharan Africa.⁵ HIPSSA does not cover the whole African continent, but has generally consistent initiatives customised for east, west, central and southern African states, via the EAC, ECOWAS, ECCAS and SADC RECs respectively, thus covering all of sub-Saharan Africa.

One aspect of HIPSSA is that 'cybersecurity' covers initiatives dealing with cybercrime, e-transactions and data protection (the same scope as the AU Convention). From this aspect of HIPSSA comes what is often called the 'SADC Model-law on data protection' (or even the 'EU/ITU Model Law'),⁶ which is also relevant to the EAC, and its ECCAS equivalent. These

³ ECOWAS Member States: Benin, Burkina Faso, Cape Verde, the Ivory Coast, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

⁴ For the history of HIPSSA, see ITU 'Support for harmonization of the ICT Policies in Sub-Saharan Africa' <<http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx>>

⁵ 'HIPSSA Project', ITU website <<http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx>>

⁶ HIPSSA Project *Southern African Development Community (SADC) Model Law on Data Protection* <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf>

Model Laws are broadly consistent with the provisions of the African Union (AU) Convention provisions, or the ECOWAS Supplementary Act, all of which start from the same EU-influenced approach. They have very detailed provisions, usually with the same substantive effect as the AU Convention, but often with very different wording.

Southern Africa (SADC)

The Southern African Development Community (SADC) encompasses 15 countries⁷ in southern and central Africa, and Indian Ocean states, six of which have data protection laws (Angola, Lesotho, Mauritius, Seychelles, and South Africa – and Zimbabwe only for its public sector), and at least three of which have current Bills (Tanzania, Swaziland and Madagascar). South Africa's new law can be expected to be a significant stimulus to laws in at least the other SADC countries because of South Africa's role as the regional economic power. There has already been work done on SADC-wide data protection laws and policies⁸, and the *SADC Model Law on Data Protection*⁹ is part of the EU/ITU HIPSSA project.

East Africa (EAC)

Less advanced in data protection developments as yet is the East African Community (EAC), a regional group of five East African countries (Kenya, Tanzania, Uganda, Rwanda and Burundi)¹⁰, where English and French are variously spoken. None have yet enacted data protection laws, but Tanzania and Kenya are both developing them. EAC has taken initiatives to encourage the member states to adopt data privacy legislation.¹¹ Such initiatives include the current discussion of a *Draft Bill of Rights for the East African Community*,¹² which (unlike the African Charter on Human and Peoples' Rights) incorporates the right to privacy. It also includes a right of legal enforcement culminating in a right of appeal to the East African Court of Justice. Also, although not binding, the EAC has adopted the *EAC Framework for Cyberlaws* Phases I and II¹³ in 2008 and 2011 respectively, addressing multiple cyber law issues including data protection. The data protection recommendations in Phase I (2008) are very brief and in general terms, merely encouraging adoption of international best practice.¹⁴ The EU/ITU 2012 'Model-law on data protection' was also aimed at the EAC countries.

⁷ SADC Member States: Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe; See SADC website at <<http://www.sadc.int/>> .

⁸ Chetty, P, 'Presentation on Regional Assessment of Data Protection Law and Policy In SADC' (PPTs) Workshop on the SADC Harmonized Legal Framework for Cyber Security Gaborone Botswana 27th February-3rd March 2012.

⁹ *SADC Model Law on Data Protection* (ITU website) <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf>

¹⁰ East African Community at < <http://www.eac.int/>>; Tanzania is a member of both EAC and SADC.

¹¹ For a more detailed account, see 'EAC initiatives' in Alex B Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31(2) *Computer Law and Security Review* (forthcoming).

¹² *Draft Bill of Rights for the East African Community*, May 2009, Arusha, Tanzania.

¹³ EAC Cyberlaws Framework <http://www.eac.int/index.php?option=com_docman&task=cat_view&gid=153&Itemid=148>; Framework for Cyberlaws, Phase II (UNCTAD, 2011) < http://r0.unctad.org/ecommerce/docs/EAC_Framework_PhaseII.pdf>.

¹⁴ EAC Cyberlaws Framework, Phase I (2008) <http://www.eac.int/index.php?option=com_docman&task=doc_download&gid=633&Itemid=148>

Central Africa (ECCAS /CEMAC)

The Economic Community of Central African States (ECCAS) has ten member states,¹⁵ which are primarily French and Portuguese-speaking, and the Communauté économique et monétaire de l'Afrique centrale (CEMAC) has six French speaking member states that are also members of the ECCAS. Of these countries Angola and Gabon already have data privacy laws, and Chad is currently developing one. ECCAS adopted, in 2013, three texts as 'model laws' and CEMAC adopted them as 'draft directives' (CEMAC), on data protection, electronic communications and cyber crime. The data protection text elaborated and adopted with the support of EU/ITU HIPSSA project is very close to the SADC model law. It contains however some particular developments of its own related to genetic data processing, while in the SADC model law developments are made on processing of medical data related to sexual life for research purposes.¹⁶

North Africa

North Africa (north of the Sahara) does not have a sub-regional institution with an active interest in data privacy,¹⁷ although Morocco (the only non-AU member on the continent) and Tunisia already have data privacy laws. Morocco was the first African country to request to accede to Council of Europe data protection Convention 108. The Tunisian Law adopted before the "Spring revolution" has been announced as being revised in the future in particular to strengthen the independency of the data protection authority and the control over public sector personal data processing. The political situation in other North African countries makes direct regional cooperation unlikely. However, for these and many of the sub-Saharan countries, the Association of Francophone Data Protection Authorities (AFAPDP) also serves as a point of contact, exchange of views, capacity building cooperation and an influence for consistency.

Content of the agreements and model laws

The extent to which these ECOWAS, SADC, ECCAS-CEMAC and EAC developments, and the 14 national data privacy laws that African countries have enacted, are consistent in their principles and enforcement mechanisms, both between themselves, and with the new AU Convention, is beyond the scope of this short article. No one has yet undertaken such a comprehensive study. Makulilo's brief analysis of the content of the AU, ECOWAS and SADC initiatives,¹⁸ makes it clear that there is a very high degree of similarity between the content of the three initiatives. He considers the content of the AU Convention and ECOWAS Supplementary Act to be identical, and the principles in the SADC Model Law to 'appear slightly different in formulations'. It is worth emphasising that they all reflect very strongly a 'European' approach to a data privacy law, which is not surprising given their history and influences. They all include numerous 'European' elements not required by the OECD privacy

¹⁵ The member countries of ECCAS, founded in 1983, are: Angola, Burundi, Cameroon, Congo, Democratic Republic of Congo, Gabon, Equatorial Guinea, Chad, and Sao Tome and Principe: see ECCAS pages, UN Economic Commission for Africa <http://www.uneca.org/oria/pages/eccas-economic-community-central-african-states-0> The CEMAC member states are Cameroon, Central African Republic, Chad, Congo, Equatorial Guinea, and Gabon.

¹⁶ ECCAS Model Law / CEMAC Directives on Cybersecurity (Data protection, e-transactions, cybercrime) (in French) <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/REGIONAL%20documents/projets_des_lois_types-directives_cybersecurite_CEEAC_CEMAC.pdf>.

¹⁷ The Arab Magreb Union (AMU), founded in 1989, and involving 5 states (Mauritania, Morocco, Algeria, Tunisia and Libya), with headquarters in Morocco, has not been involved in data protection: see AMU pages, UN Economic Commission for Africa < <http://www.uneca.org/oria/pages/uma-arab-maghreb-union-0>>. Nor is the much larger Community of Sahel-Saharan States (CEN-SAD): see < <http://www.uneca.org/oria/pages/cen-sad-community-sahel-saharan-states>>.

¹⁸ '3. Harmonisation of data privacy policies' in Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa',

Guidelines, such as the requirement of a DPA with important powers, the necessity of legitimate processing, restrictions on direct marketing, special protections for sensitive information and automated processing, and the data-subject's right of objection to processing.

Given this overall high level of consistency of relatively strong protections, it is surprising that Makulilo argues that this consistency is undermined by important differences in such areas as data exports and jurisdictional issues, to the extent that he concludes that 'the harmonisation initiatives do not seem to point toward a common direction,' and even that they may be 'counterproductive and at best will create barriers to the free flow of personal information within and across RECs'.¹⁹ While accepting that there are difference in data export principles and in some other areas, our expectation is that these are likely to be less significant than the overall high degree of consistency, and that if any of these conventions and model laws are followed as the basis for new national laws in Africa (or revision of existing laws) then this will advance Africa-wide harmonisation of data protection, and at a relatively high level.

Conclusions: The international context of African harmonisation

While the general understanding is that 'globalisation' means adoption of universal standards, in practice when personal data processing is concerned it means a lot of regional developments, north-south data flows and some growing global hegemonies. In that sense, seeing data protection law being promoted in parallel at the national level and by way of model laws on the sub-regional level, when complete regional (i.e. Africa-wide) integration is not achieved, is a very pragmatic and pedagogical way of promoting consistent legal systems and knowledge in a new field on a large scale.

The early initiative of a binding agreement by ECOWAS, which was the first sub-region to act, echoes the strategy the EU took with the adoption of the EU Directive of 1995. From the African Union (AU) level, adopting a convention seems also logical while the global level is yet to be also reached. When taking into account the universal nature of the DP principles including the rights of data subjects, one can expect in the coming years more harmonized DP practices in different sectors in Africa. This will be due in significant part to the influence of these agreements, and also the influence of exchanges and cooperation within the networks of DPAs, and sometimes some tensions among them where criteria for the applicable law or interpretations may differ.

We can also expect that the international legal battles that are apparent recently between Europeans and US firms will tomorrow involve also Africans on their continent. So long as the United Nations does not move toward achieving a global convention, it is likely that links will continue to strengthen between those in charge of data protection in Africa and the Council of Europe's administration of data protection Convention 108. This may occur formally, as new African parties accede to the Convention (as Morocco and Mauritius are moving to do), or informally because African States with data protection laws and organisations are invited as observers to the work on the modernization of that Convention or its operation.

¹⁹ '5. Conclusion'. In Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa'.