University of New South Wales Law Research Series

COMPARING AFRICAN DATA PRIVACY LAWS: INTERNATIONAL, AFRICAN AND REGIONAL COMMITMENTS

GRAHAM GREENLEAF & BERTIL COTTIER

[2020] *UNSWLRS* 32

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

Comparing African data privacy laws:
International, African and regional commitments

Graham Greenleaf and Bertil Cottier* - 20,447 words (with Tables)

Pre-print version 22 April 2020; Submitted to *International Data Privacy Law* (OUP)

Comments are welcome to graham@austlii.edu.au or bertil.cottier@usi.ch

* Authors: Graham Greenleaf is Professor of Law & Information Systems at UNSW Australia. Bertil Cottier is Professor of Communication Law at the University of Lugano (Switzerland). Valuable comments and criticisms have been received from Marie Georges, Ian Brown, Sophie Kwasny, Alice Munyua, Drudeisha Madhub, Gabriella Razzano , Enrico Callandro and Pat Walshe, but responsibility for all content remains with the authors. Special thanks go to Marie Georges, a pioneer of data protection in both Europe and Africa. Earlier versions of parts of this article have previously appeared in G. Greenleaf and M. Georges (2014) 131 *Privacy Laws & Business International Report,* 18-21, and (2014) 132 *Privacy Laws and Business International Report* 19-21, December 2014.

1. Introduction

At various times over the past 50 years of enactment of data privacy laws, differing regions of the world have become the most active 'growth areas' in the global diffusion of data privacy laws, now found in 143[1] countries. This was so for Western Europe in the 1970s and 1980s, Latin America in the 1990s (with the constitutional 'habeas data'), Eastern Europe also in the 1990s and early 2000s (as part of its post-Berlin-Wall democratization, and preparations for EU membership), and Asia in 2010-13.[2] Now it is Africa that is leading global expansion, with 12 countries since 2013 adopting new laws.

Fifty-eight percent of all African countries – thirty-two of the 55[3] – have enacted data privacy laws[4] as at February 2020.[5] African countries have regularly enacted data privacy laws for nearly twenty years, in Cape Verde (2001, amended 2013), Seychelles (2003), Burkina Faso (2004, under revision), Mauritius (2004, revised 2017), Tunisia (2004, under revision), Senegal (2008, under revision), Benin (2009 revised 2017), Morocco (2009, under revision), Angola (2011), Gabon (2011), Lesotho (2011), Ghana (2012), Ivory Coast (Cote d'Ivoire, 2013), Mali (2013), South Africa (2013), Madagascar (2014), Chad (2015), Malawi (2016), Equatorial Guinea (2016), Sao Tome e Principe (2016), Guinea (Conakry) (2016), Mauritania (2017), Niger (2017), Algeria (2018), Botswana (2018), Nigeria (2019), Uganda (2019), Kenya (2019), Congo-Brazzaville (Republic of Congo) (2019), Togo (2019) and Egypt (2020) plus Zimbabwe (2002) which covers the public sector only.[6] About half of these laws are not yet in force, or not fully effectively so due to lack of appointment of a data protection authority (DPA). There are 54 European jurisdictions with data privacy laws: 47 Council of Europe member States, plus 7 other territories[7], so of the 89 non-European countries with data privacy laws, 36% (32) are from Africa. Of the whole 143 jurisdictions with data privacy laws, 22% are from Africa.

At least a further five African countries have official Bills under consideration.[8] That leaves 18 (33%) of the 55 African countries where no laws or Bills for data privacy laws are known.[9] Other than Europe and Central Asia, Africa has the highest proportion of countries with data privacy laws in any major region of the globe.[10]

---

[1] As at 19 February 2020 there are 142 countries with data privacy laws: 132 of them are detailed in Greenleaf, G 'Global Data Privacy Laws 2019: 132 national laws and many bills' (2019) 157 *Privacy Laws & Business International Report* 14-18 and accompanying Table; A further 10 countries were added by the end of 2019: see G. Greenleaf and B. Cottier '2020 ends a decade of 62 new data privacy laws' (2020) 163 *Privacy Laws & Business International Report* 24-26. Since then, Egypt has enacted its law in February 2020.

[2] 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>.

[3] The African Union lists 55 countries as members <https://au.int/memberstates> , including Western Sahara (Sahrawi Arab Democratic Republic), the statehood status of which is disputed between Morocco and the Polisario Front, and it is not a UN member State. We have included it because it has African Union membership. We have not included some very small island territories of European countries, such as Saint Helena, Ascension & Tristan de Cunha, a UK overseas territory, and Reunion island, a French territory.

[4] The definition of a 'data privacy law' used in this article is that explained in Greenleaf 'Sheherezade and the 101 data privacy laws' (2014), and is essentially that of a national law covering all or almost all of the private sector (and/or the public sector), embodying all or almost all of the principles included in the first generation of international privacy standards (OECD Guidelines 1980 and Council of Europe Convention 108, 1981), plus some method of enforcement by law.

[5] These laws are listed in the Table in the Appendix.

[6] Many of the first data privacy laws outside Europe were initially 'public sector only' (eg Australia, Korea, Japan and Taiwan), until they late enacted private sector reforms, so we have included Zimbabwe.

[7] Jersey, Guernsey, Isle of Man, Greenland, Faro Islands, Kosovo and Gibraltar.

[8] These Bills are detailed in part 2.2.

[9] See part 2.3, for factors contributing to the absence of laws or Bills.

[10] By comparison with the Caribbean, Latin American, Asian,, Middle Eastern and Pacific Island regions.

As well as these national laws and Bills, in Africa there is an African Union Convention on cyber-security and data protection that potentially spans the whole continent, plus regional multi-state data privacy instruments, and a civil society Declaration. African countries have also been among the first to apply and be accepted to accede to Council of Europe data protection Convention 108. All of these factors, and others, must be taken into consideration in an overall account of data privacy developments in Africa.

There have been few comparative studies of African national data privacy laws and their relationships to African multi-national data privacy agreements, nor to international standards and commitments. The most extensive studies are those edited by Alex Makulilo[11] (2016), where the focus is on developments in individual countries, and the monograph by Mouhamadou Lo[12] (2017), which is more explicitly comparative. A significant new digital comparative initiative, 'Data Protection Africa', [13] is developing pan-African resources. These pioneering works are complemented by other[14] analyses of individual laws in each country, their histories and national particularities, and are essential for a full understanding of privacy developments in Africa. In this study we are taking a somewhat different approach, with a focus on direct comparison of (first) the principles or standards found in international, pan-African and African regional data privacy agreements, and then (second) the principles or standards enacted in each of the 32 current laws. The relationships between the agreements and the national laws will be analysed.

In this first article, we commence by outlining the distribution of national laws across Africa, and the relationships between the countries concerned (regional associations of countries) and their data protection authorities (associations of DPAs), and the national constitutional provisions relevant to privacy protection. Then we will compare international (primarily European) privacy principles and standards with both the Africa-wide (African Union) privacy commitments and standards, and the regional standards established in various African RECs (Regional Economic Communities). Possible influences on development of national privacy laws in Africa will then be suggested, to be examined against the evidence of these national laws in the second article.

The second article will examine and compare each of the national data privacy laws at a more granular level. Each of the 32 laws will be assessed against over 30 standard features of data privacy laws (based on three generations of international data privacy standards), with any additional features being noted.

We refer to the national laws and international agreements we are discussing as 'data privacy' instruments. We prefer this to 'data protection' (common in Europe, originating in Germany), or the French preference for a broader reference to 'information and liberties', or simply 'privacy'. We agree, however, that data privacy laws do often protect other liberties, not only privacy (and we intend that broader meaning), and do not protect some aspects of human conduct regarded as 'private' but which are not to do with data.

1.1. An African approach to data privacy or privacy laws?

From the literature concerning privacy and privacy laws in Africa, no strong argument emerges that there is some distinctively African conception of privacy or approach to the

[11] Alex Makulilo (Ed) *African Data Privacy Laws* (Springer, 2016).

[12] Mouhamadou Lo *La protection des données à caractère personnel en Afrique* (Baol Editions, 2017). Lo was the first president of the Senegalese data protection commission, and an influential expert concerning the ECOWAS Supplementary Act and the AU Convention (discussed later).

[13] Data Protection Africa <https://dataprotection.africa/>, developed by ALT Advisory, provides information on data protection laws and access to data protection authorities in 32 African countries (not identical with the 32 listed above). It includes brief Fact Sheets on each country, entries on case law and legislative trends, and directories of organisations involved in data protection, including content in 18 languages.

[14] The collection edited by Makulilo includes studies of developments in 20 countries, each averaging around 20 pages.

development of data privacy laws. It is often argued that, at least until recently, African societies across the continent placed a stronger emphasis on communitarian or collectivist values (sometimes referred to as *Ubuntu*) than on individualistic values. From a survey of studies of collectivist values across Africa, Makulilo concludes that such values are in retreat in the face of the globalisation of western culture, particularly since the collapse of the socialist bloc, with more individualistic values becoming predominant.[15] He argues that the concept of privacy only developed in Africa at the end of the colonial period, particularly as outgoing colonial powers often left constitutions providing protections to privacy among other values, even though this may have been inconsistent with the more collectivist values of those societies at that time.[16] 'Despite the emerging data privacy policies in the continent, there is as yet no philosophical conception of the term privacy in the African context', Makulilo argues.[17] The most widely cited African academic analysis of privacy, also adopted in South African court decisions, is by Professor Neethling.[18] As Makulilo notes, it is a version of Western liberal information control theories, founded on individuality and autonomy.[19] His conclusion is that the increasing claims for privacy in Africa are 'due to an increased use in modern technologies by both individuals and institutions', as well as being influenced by 'trading and business considerations with European countries,' [20] and that globalisation is changing Africa in the direction of more individual autonomy. Increased urbanisation, and the penetration of western media, are part of these processes.[21] In relation to development of data privacy and other IT-related legislation, the influence of international funding sources should also not be ignored.

In this article, we are only examining data privacy (or data protection) national legislation, and international and African agreements concerning such legislation, plus looking at the question of whether there is constitutional support for such data privacy protections. We do not examine whether general civil law protections (common law, civil law, Roman-Dutch law etc) in African countries, or other aspects of their constitutional law, provide protections to privacy which have distinctive African elements. Questions of whether there is an African understanding of foundational rights, and whether it is reflected in these aspects of national laws, are not addressed by this article. The African Charter on Human and Peoples' Rights (discussed in part 3.5) also provides a continental foundation for the protection of liberties broader than data privacy.

The absence of arguments for an 'African approach to privacy' in relation to data privacy legislation has a parallel in the failure of arguments that 'Asian values' (particularly of communalism) meant that data privacy laws would not take root in Asia, or would have distinct characteristics from different Western countries.[22] Asian countries, like those in Africa, are increasingly enacting data privacy laws, and those laws adhere closely to European models of data privacy laws.

---

[15] Makulilo, pp. 10-15.

[16] Makulilo, pp. 15-16; Makulilo considers this may have been in part to protect remaining settler populations.

[17] Makulilo, pp. 17-18.

[18] J. Neethling (2005) 122(1) 'The Concept of Privacy in South African Law' *South African Law Journal*, 18-28; See discussion in A. Roos 'Data protection law in South Africa' in Makulilo (Ed) *African Data Privacy Laws*).

[19] ibid

[20] Makulilo, p. 21.

[21] Makulilo, pp. 14-15.

[22] G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 17-18; 561-2.

In surveying the development of data privacy legislation in Africa, we therefore cannot expect to find (i) a lack of interest in enacting such laws, or (ii) a distinctively African approach to such laws. This leaves open whether we will find (iii) great diversity between national laws; (iv) consistency arising from standards developed in Africa; (v) regional consistencies within Africa due to regional trading blocs, with differences reflecting colonial influences; or (vi) strong influence of standards arising from outside Africa. These external influences could, for example, be from the strongest global economic influences: the USA (sectoral laws; lack of a data protection authority (DPA)), China (data localisation; weak principles; no DPA), or Europe (strong principles; DPA with strong powers).

2. National laws and Bills in Africa

We start with a sketch of the legislative position in each of the 55 African countries. The Legislation Table discussed in part 2.1 includes those countries with principal laws enacted by a legislature and signed into law which meet our criteria for a data privacy law (or in the case of Nigeria, a regulation at present); the Bills for proposed data privacy laws, discussed in part 2.2, are either Bills introduced into legislatures, or as official government proposals; and part 2.3 discusses those African countries where there is no data protection law or bill that satisfies the basic criteria for a data privacy law.

2.1. Legislation in African countries

The 31 data privacy laws in Africa are shown in the Table in the Annexure, with details of the name of the law, years of enactment and most recent major amendments, the name of the data protection authority (DPA) created and whether it has been appointed. Also listed are the regional organisations relevant to privacy of which the country is a member, any privacy-related international agreements to which it is a party, and any associations of data protection authorities of which its DPA is a member.

The Table demonstrates some of the basic features of the national laws, some of which require some comparative comments here, and others of which will be referred to later. Almost all the laws enacted in Africa have been brought into force, other than those very recently enacted, such as in Algeria. The long-standing exception of a law not yet in force is from the Seychelles (2003), for reasons uncertain.[23] More significantly, South Africa (2013) after seven years has an Act which is only partly in force, and an inactive DPA as a result, although it was expected (prior to the pandemic) to be brought fully into force very soon.[24]

All African laws are comprehensive of both public and private sectors, the one exception being Zimbabwe (2002, public sector only, but a comprehensive Bill since 2013). Comprehensive laws are the rule in most other regions, with Asia exceptional (private-sector-only laws in Singapore, Malaysia, Vietnam and China, with India and Indonesia enacting Bills to change that position).

Appointment (and non-appointment) of DPAs

Almost all of the African data privacy Acts allow for the appointment of a data protection authority (DPA), separate from any Ministry (exceptions are in Nigeria and Uganda and (pending a second law) Congo-Brazzaville), which is regarded widely as an essential element

[23] A Makulilo 'Data protection of the Indian Ocean Islands: Mauritius, Seychelles, Madagascar', [13.2.4] (in Makulilo (Ed) *African Data Privacy Laws*) does not give any reasons. Nor do other publications.

[24] Sizwe Snail, Commissioner, Information Regulator, said that the 2013 Act will enter into force in the second quarter of 2020 (Report of speech at CPDP conference, Brussels, 23 January 2020).

of an effective data privacy law.[25] Separate DPAs often also have statutory guarantees of independence, but this is sometimes not the case (for example, Ministerial instructions are allowed in Botswana). In some regions of the world a model of enforcement by Ministries with sectoral responsibilities, rather than a separate DPA, still has a few adherents, but these are disappearing. In Asia only Vietnam, China and Taiwan adhere to this model, with other civil law countries having adopted DPAs (Japan, Korea, Thailand), or proposing to do so (Indonesia and India).

However, no DPAs have yet been appointed in 15/32 countries with laws: Seychelles (since 2004), Angola (since 2011), Chad, Equatorial Guinea, Madagascar, Guinea (Conakry), Mauritania, Niger, Algeria, Botswana, Togo, Kenya, Uganda, Congo-Brazzaville and Egypt. In the last seven of these, the legislation was only enacted in 2018 or later (see the Table in the Appendix). Two years to bring an Act into force, appoint a DPA and provide it with some resources, is (in our opinion) a reasonable allowance of time, though there is no international standard for this. So eight of the 15 countries with laws are open to criticism on this ground. Failure to appoint in due time a DPA has been repeatedly criticized for being a major impediment to effectiveness of the data protection legislative frameworks.[26] This delay occurs more often in Africa than elsewhere, but that is explained in part by the large number of recent African laws.

On the other hand, to the credit of African legislatures, it should be underlined that all existing DPAs enjoy the status of independent agencies, except for in Morocco (under direct supervision of the Prime Minister), and in Algeria.[27] In the past three years, Mali, Ivory Coast and Cape Verde have appointed DPAs.

African enactment of data privacy laws is not static, with three countries having now enacted stronger 'second generation' laws (Cape Verde, Mauritius, and Benin), and Bills progressing slowly in Tunisia, Burkina Faso and Morocco. As detailed in the second article in this series, these amended laws are now much closer in standards to the EU's GDPR, often more so than recent new laws.

The most significant new laws are in Nigeria, the largest sub-Saharan African economy by GDP,[28] which until 2019 only had sectoral laws for credit reporting and electronic communications 'guidelines',[29] in Kenya, where the Act emerged from lengthy debate and competing Bills as one of the most progressive English-language data privacy laws in Africa,[30] and in Egypt, the third most populous African country, and one of the most influential.

---

[25] See C. Bennett and C. Raab *The Governance of Privacy* (MIT Press, 2006), p.134; G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 73-75.

[26] Among others Joao Luis Traça and Bernado Embry 'An overview of the legal regime for data protection in Cape Verde' (2011) 1(4) *International Data Privacy Law* 249-255 and Lo, op. 232;

[27] Details of indicia of independence are in the second article of this series.

[28] Nigeria's GDP is ranked at 30 in the world, whereas that of Egypt is ranked at 29.

[29] It was argued by Aderibigbe that prior to 2019 Nigeria has legally binding data privacy 'guidelines' (NITDA Guidelines on Data Protection), for the public and private sectors. We do not consider them a data privacy law because they only apply to electronic communications, individual rights such as correction are absent, and their enforceability may be questionable. Evidence of enforcement or compliance is not apparent. See Ngozi Aderibigbe 'Nigeria Has a Data Protection Regime' 12 December 2017 http://www.jacksonettiandedu.com/nigeria-has-a-data-protection-regime/; see also I S Nwankwo 'Information Privacy in Nigeria' pp. 59-60 (discussing the draft Guidelines) in A Makulilo *African Data Privacy Laws*. NITDA issued a new, more comprehensive and enforceable Regulation in 2019 which does qualify as a data privacy law: · G. Greenleaf 'Nigeria regulates data privacy: African and global significance' (2019) 15*8 Privacy Laws & Business International Report* .

[30] See Greenleaf and Cottier '2020 ends a decade of 62 new data privacy laws'.

2.2. Official Bills in African jurisdictions

Five African countries are known to have official data privacy Bills, whether introduced in the legislature or merely made public by the government, with some developments having taken place in the last five years. The five countries, large and small, are:

- **Ethiopia** has had various draft Proclamations (the highest form of Ethiopian legislation) on data protection in 2009 and 2014. In April 2020 a new draft Personal Data Protection Proclamation was released, with strong GDPR influence.
- **eSwatini** (Swaziland) has had a Data Protection Bill under consultation since 2013.
- **Tanzania** has had a draft law before Cabinet since 2017.
- **Zambia**'s Data Protection (Repeal) Bill, 2018 was approved by Cabinet in June 2018, to replace the Electronic Communications and Transactions Act, No. 21 of 2009. Zambia has signed the AU Convention.
- **Comoros** has had a data protection Bill since 2014, and may have enacted it in 2016 according to one source,[31] but evidence of enactment has not been found. Comoros became a signatory to the African Union cybercrime and data protection Convention ('AU Convention') in 2017.

2.3. African countries with no laws or Bills

There are still 18 African countries with no data privacy laws or official Bills (within the last five years), about 30% of African countries. Only a few are surprising because of relatively high GDP per capita (Namibia) or governments with a strong interest in technology (Rwanda[32]). Some do not have official Bills but are known to actively involved in policy development. For example Gambia is receiving assistance from the Council of Europe,[33] and Namibia has held a drafting workshop in February 2020.

Of these eighteen, most are members of one of the Regional Economic Communities (RECs) with data privacy standards or agreements which may influence them (see section 5 on RECs). If the ECCAS and CEMAC RECs gain more momentum in relation to data privacy, this could be a significant influence on four central African member countries (Cameroon, Central African Republic, Democratic Republic of Congo and Rwanda). Similarly, ECOWAS and its Supplementary Act are likely to influence its four remaining west African member states, (Gambia, Sierra Leone, Liberia and Guinea Bissau), to enact laws. That leaves EAC member Burundi (under EU sanctions for anti-democratic and human rights abuses), SADC members Namibia and Mozambique, and the disputed territory of Western Sahara (Sahrawi Arab Democratic Republic). The remaining six are countries in Africa's north and north-east afflicted by regional or civil wars or very repressive governments (Libya, Sudan, South Sudan, Eritrea, Djibouti and Somalia), and with no REC to influence them (except for South Sudan which is an EAC member).

One anomaly is that two ECOWAS members (Guinea-Bissau and Sierra Leone) have already signed the AU cybercrime and data protection Convention, even though they have no data privacy law or Bill. If that Convention is ratified they will have an obligation under international law to enact a law (although they already are, under the ECOWAS

---

[31] Mouhamadou Lo *La protection des données à caractère personnel en Afrique* (Baol Editions, 2017).

[32] An ICT law - Loi N°24/2016 du 18/06/2016 régissant les Technologies de l'Information et de la Communication – establishes Rwanda Utilities Regulatory Authority (RURA), and has some elements of a data privacy law, but its privacy-invasive elements are condemned by Article 19 (Article 19 'Rwanda: 2016 Law Governing Information and Communication Technologies' Legal Analysis, May 2018).

[33] Council of Europe, Newsroom 'Privacy Policy in The Gambia' 10 May 2019 <https://www.coe.int/en/web/data-protection/-/privacy-policy-in-the-gambia>

Supplementary Act). Congo-Brazzaville (Republic of Congo) was in that category but has enacted a law.

Future prospects

New African laws have been enacted at a rate of 3.5 per year in 2016-19, and at a rate of 2.4 per year since 2010. The enactment of the EU GDPR in 2016, and it being in force since May 2018, is the most obvious impetus to countries which have been drafting and considering draft data privacy laws for some years to start legislative debates, fourteen of which resulted in enactment of legislation in 2016-19. The impact this has had on enactment of 'GDPR-like' provisions in those laws will be explored further in the second article in the series. The small number of ratifications of the AU Convention (discussed below) indicates that it has not been a significant impetus.

There are 23 African countries remaining with no laws, five of which do have Bills. Even if the rate of enactment of new laws reduces to two per year, it seems realistic to expect that by the end of the 2020s there will be few if any African countries that have not enacted a data privacy law. Outside Europe, some other regions might reach a similar result within five to ten years: Latin America, the Caribbean, Asia and Central Asia.[34] By this basic measure, Africa is likely to remain a leader in the enactment of data privacy laws. However, both the quality of its laws, and their enforcement, are different issues, taken up in the second of these articles.

2.4. Constitutional and other provisions

The constitutions of only seven African countries contain a specific provision on personal data protection. Most countries (28/54) however list the right to privacy among the fundamental rights and freedoms guaranteed by their constitution[35]. In addition twelve other constitutions specifically protect secrecy of communications[36]. Finally seven constitutions do not make any explicit reference to privacy matters,[37] but most of these do include the 'right to life' or 'the right to liberty'[38] expressions which in India's epochal *Puttaswamy* decision were held to be the basis of an implied constitutional right to privacy.[39] A subsequent Indian Supreme Court decision declared a colonial era s. 377 of the Penal Code criminalising gay sex as unconstitutional on this basis [40] Botswana's High Court, citing this authority, held unconstitutional (*ultra vires* the Constitution) two similar Penal Code provisions criminalising gay sex, which had been copied s. 377, with the 'right to liberty' in Botswana's Constitution being one of the grounds.[41] In South Africa, the concept of dignitas has been a foundation of

---

[34] G. Greenleaf 'Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)' (2019) Supplement to 157 *Privacy Laws & Business International Report* (PLBIR) 16 pgs. <https://ssrn.com/abstract=3380794 >.

[35] Burkina Faso (art.. 6), Burundi (art. 23), Chad (art 17), Congo (Democratic Republic) (art. 31), Egypt (art. 57), Eritrea (art. 18), Ethiopia (art. 26), Guinea (art. 12), Guinea Bissau (art. 44), Kenya (art. 31), Lesotho (art. 4), Liberia (art. 16), Lybia (art. 12), Malawi (art. 21), Mali (art. 6), Mauritania (art.13), Morocco (art. 24), Namibia (art. 13), Nigeria (art. 37), Rwanda (art. 23), Sao Tome and Principe (art. 23), Sierra Leone (art. 15), South Africa (art. 14), South Sudan (art. 22), Sudan (art. 37), Tanzania (art. 16), Uganda (art. 27) and Zimbabwe (art. 57).

[36] Benin (art. 21), Cameroon (preamble), Central African Republic (art. 18), Congo (art. 26), Djibouti (art. 13), Equatorial Guinea (art. 1), Gambia (art. 23), Ghana (art. 18), Madagascar (art. 13), Niger (art. 29), Senegal (art. 13) and Togo (art. 29).

[37] Lack of constitutional references: Botswana (only privacy of the home), Comoros, Ivory Coast, Mauritius, Somalia, Swaziland and Zambia.

[38] For example, Constitutions of Botswana, ss. 3-5, Swaziland, ss. 14-16, Mauritius, ss. 3-5, Zambia, ss. 11-13.

[39] *Justice K.S. Puttaswamy (Retd.) v. Union of India* 2017 (10) SCALE 1.

[40] *Navtej Singh Johar v Union of India Ministry of Law and Justice Secretary* [2018] INSC 746 <http://www.liiofindia.org/in/cases/cen/INSC/2018/746.html >

[41] *Motshidiemang v Attorney General (Lesbians, Gays and Bisexuals of Botswana (LEGABIBO), Amicus Curiae)* (2019) High Court of Botswana, 11 June 2019 MAHGB-000591-16. In Botswana's Constitution, ss 3 and 9 explicitly protect only the privacy of property, and privacy against bodily searches.

the protection of privacy, in both constitutional law and civil law.[42] Of even greater likely importance are the constitution provisions, and judicial interpretations, in European countries from which these African provisions are very often derived. The potential for similar interpretations in Africa is beyond the scope of this article, and is unlikely to be uniform.[43] The extent to which constitutional protections are justiciable will also vary between countries. However, it should be clear from this brief survey that in most African countries there is considerable potential for constitutional protection of privacy and related liberties. However, as Makulilo points out, there is as yet little case law based on constitutional protections of privacy in Africa.[44]

The seven states which have adopted a constitutional provision dedicated to data protection (Algeria, Angola, Cape Verde, Gabon, Mozambique, Seychelles and Tunisia[45]) do not display homogeneity: the relevant norm(s) are very different both formally and substantially. The constitutions of Algeria (art. 46), Angola (art. 32) and Gabon (art. 1.6) just command their respective parliaments to enact data protection laws without further instructions regarding the content of these laws. The constitutions of Seychelles (art 28) and Mozambique (art. 71) go beyond a mere mandate to legislate and directly guarantee some key elements of data protection like the right of access, the principle of purpose limitation (Seychelles), the prohibition to process sensitive data as well as the right of correction of inaccurate data (Mozambique). The constitution of Tunisia (art. 24) mentions protection of personal data as a substantial right alongside protection of privacy and secrecy of telecommunications. Diversely, the exceptionally dense constitutional provisions of Cape Verde (art. 45 and 46) enshrine most fundaments of data protection from a full fledged right of access to a prohibition of the use of an unique identification number.

Finally, it should be stressed that the lack of explicit constitutional provision protecting personal data or private life does not preclude the adoption of a robust data protection law: Ivory Coast and Mauritius, whose constitutions do not explicitly mention privacy, have enacted data protection laws which are among the most progressive in Africa. On the other hand, Mozambique, though having a remarkable constitutional protection of data protection, has not followed up with legislation.

A full assessment of the general legal protections of privacy in a jurisdiction, even if it does not encompass sectoral legislation, should also consider whether there is general civil law protection of privacy (by a statutory 'right of privacy', or one in the civil code,[46] or by a general tortious or equitable right), or general protection provided through criminal law.[47] Those considerations are beyond the scope of this article. South Africa is an example of a country with extensive common law protection of privacy interests, much of it derived from

[42] See for example *NM and Others v Smith and Others* [2007] ZACC 6 <http://www.saflii.org/za/cases/ZACC/2007/6.html>

[43] In Kenya, a case similar to Botswana did not succeed: Max Bearak "'Not a fashion statement': Botswana legalises gay sex" *Sydney Morning Herald* 12 June 2019 < https://www.smh.com.au/world/africa/not-a-fashion-statement-botswana-legalises-gay-sex-20190612-p51ww3.html>

[44] Makulilo, p. 20.

[45] The constitution of Gabon and Mozambique limit protection to automatically processed data, Seychelles to data processed by public authorities.

[46] For example, *Civil Code* (Mauritius), art. 22.

[47] For example, see the analysis of constitutional, civil and criminal protections in all Asian countries in Greenleaf *Asian Data Privacy Laws* (OUP, 2014)

Roman-Dutch law.[48] The broader question of the strength of the rule of law in a particular country, is also beyond consideration here.

3. International data privacy commitments of African countries

African states have some data privacy obligations that originate from outside Africa, which need to be taken into account in an assessment of all the factors influencing African national data privacy laws.

3.1. The ICCPR and other UN instruments

The International Covenant on Civil and Political Rights (ICCPR), art. 17 of which recognizes the right to privacy, has been ratified by all African states,[49] with the exception of Comoros[50] and South Sudan. The number of African countries having ratified the 1st optional Protocol, which allows individuals to submit complaints ('communications') to the Human Rights Committee, is lower (36) because 19 African countries have not ratified this text.[51] Only four complaints against African countries concerning privacy issues have been made.[52] Other UN instruments concerning privacy do not impose additional obligations on member states.[53]

3.2. Data protection Convention 108/108+ (Council of Europe)

Data protection Convention 108, a Council of Europe convention since 1981, has standards approximating those of the EU's data protection Directive of 1995, but phrased in more general terms. In 2018 it has completed a 'modernisation' process resulting in a new version of the Convention ('108+'), open for signature in October 2018, which includes many but not all of the innovations in the GDPR, and can be described as 'GDPR Lite'.[54]

Since 2011 the Convention's Consultative Committee and the Council of Europe have been actively seeking to 'globalise' the Convention, promoting accession to it by states outside Europe. At present, in addition to its 47 European parties, eight countries outside Europe are now Parties (by chronological order of accession): Uruguay, Mauritius, Senegal, Tunisia, Cape Verde, Mexico, Argentina and Morocco. Burkina Faso, having been invited to accede, is still entitled to do so. African countries were 6 of the first 8 invited to accede, and 4 of the first 5 who did accede, so the 'globalisation' of Convention 108 was initially a largely African development. Opinions by the Consultative Committee to Convention 108[55] provides detail of the content of each acceding country's law (and to some extent, enforcement of the law).[56] All

---

[48] A Roos 'Data Protection Law in South Africa', Chapter 9 in Makulilo (Ed) *African Data Privacy Laws* (Springer, 2016), pp. 189-227 at pp. 196-200.

[49] Choose ICCPR from the 'Interactive dashboard' at <https://indicators.ohchr.org/>

[50] Comoros signed the ICCPR in 2008. South Sudan did neither ratify nor sign.

[51] Has not signed: Botswana, Burundi, Comoros, Egypt, Eritrea, Ethiopia, Gabon, Kenya , Mauritania, Morocco, Mozambique, Nigeria, Rwanda, South Sudan, Sudan, Swaziland, Tanzania and Zimbabwe. Signed but not ratified: Liberia.

[52] See UNHRC Jurisprudence database at <https://juris.ohchr.org/search/results>. There have been three complaints against the Democratic Republic of the Congo, and one against Cameroon.

[53] For details see G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 38-9, 547-8.

[54] G. Greenleaf "Modernised' data protection Convention 108+ and the GDPR' (2018) 154 *Privacy Laws & Business International Report* 12-13.<https://ssrn.com/abstract=3279984>.

[55] For example, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS NO. 108] *Kingdom of Morocco - request to be invited to accede to Convention 108*, 18 October 2012, T-PD(2012)09rev

[56] Graham Greenleaf 'Uruguay starts Convention 108's global journey with accession' (2013) 122 *Privacy Laws & Business International Report*, 20-23 < http://ssrn.com/abstract=2280121>, section 'The second non-European accession invitation: Morocco'.

of the above African Parties participate in Convention 108's Consultative Committee. Burkina Faso only participates as Observer as yet.

As a further sign of the Convention's globalization, the election of the first member of the Convention's Bureau from outside Europe, Ms Awa Ndiaye of Senegal, occurred in 2018. There are a number of implications of this African engagement in Convention 108. First, African countries are being recognized as having laws meeting high international standards (until 2018, standards approximating those of the 1995 EU Data Protection Directive, though not necessarily in relation to enforcement). Second, parties to Convention 108 have an obligation to allow free flow of personal information (unrestricted data exports) to other Convention parties, and they obtain a reciprocal obligation in return,[57] although these are obligations that can only be enforced by diplomatic means.

Africa is therefore playing a significant role in the conversion of Convention 108 into a global Convention, with five of the eight non-European parties coming from Africa (Mauritius, Morocco, Senegal, Tunisia, and Cape Verde), and four other countries as Observers (Burkina Faso, Gabon, Ghana, Sao Tome and Principe). Future accessions (other than by Burkina Faso) will have to be to the higher standards of Convention 108+. The second article in this series will indicate which laws, and their enforcement, in other African countries (if any) make accession to Convention 108+ feasible, despite its higher standards.[58] In part 6, Table 3 we show that there is relatively little correspondence between the three African multinational instruments and the higher standards of Convention 108+.

An additional question is how the African Union itself is likely to be integrated into data protection agreements of global scope. The modernised Convention 108+, will be open to accession by an 'international organisation' (art. 27) invited to accede, just as it is currently open to accession by third countries. It is possible that the monitoring mechanism to be set up for the AU Convention (Art. 32(g)) would support this. The African Union could already become an Observer under the existing Convention 108.

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.[59]

3.3. European Union adequacy assessments

Assessments by the European Union that an African country's laws provide 'adequate' protection to personal data originating from the EU will facilitate trade between the EU and African countries and are likely to be regarded as very valuable. No African country obtained a positive assessment of the 'adequacy' of their data protection system from the European Union ('EU adequacy') under the 1995 data protection Directive,[60] and none are known to have so applied, although the EU did carry out some unilateral assessments.[61] Adequacy

[57] EU countries have not observed this 'free flow' requirement, because the 1995 EU Directive imposes an obligation with a higher standard limiting data exports to countries with 'adequate' laws. This 'exception' is recognized in Convention 108+.

[58] For an explanation of what is required for accession to Convention 108+, and the uncertainties involved in such an assessment, see G. Greenleaf 'How far can Convention 108+ 'globalise'?: Prospects for Asian accessions' (February 3, 2020) <https://papers.ssrn.com/abstract_id=3530870>

[59] ADPL CITATOPM

[60] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>

[61] In 2010, the European Commission unilaterally commenced evaluations of the adequacy of four African data privacy laws (Burkina Faso, Mauritius, Tunisia, and Morocco). The evaluations were conducted by the Centre de Recherche Information, Droit et Société (CRID) <http://www.crids.eu/>, University of Namur, Belgium. None of the four evaluation proceeded to a formal finding. However, Makulilo obtained and analysed the CRID 'expert reports' (Alex B Makulilo 'Data Protection Regimes in Africa: too far from the European 'adequacy' standard?' (2013) 3(1) *International Data Privacy Law* 42-50) concluding that,

assessment must now be made under the General Data Protection Regulation (GDPR).[62] Mauritius has commenced informal discussions with the European Commission concerning adequacy, but a formal assessment process has not yet commenced. In part 6, Tables 3 and 4 show that the three African multinational instruments require national enactments of very few of the higher standards of the GDPR. The question of whether recent national laws in Africa do go closer to meeting GDPR standards, even though African multilateral agreements do not require this, is addressed in the second article in this series.

4. Africa-wide data privacy commitments and standards

This section gives an overview and analysis of the 2014 African Union Convention relevant to data protection, and other pan-African privacy developments. The following section 5 does similarly at the level of the African Regional Economic Communities (RECs), with emphasis on the two regional data protection instruments of importance: in West Africa, the ECOWAS *Supplementary Act on Personal Data Protection Within ECOWAS* (2010), and the Southern African Development Community (SADC) *Model Act on Data Protection* (2013). In section 6 the relationship between the evolution of successive data privacy standards in Europe and these three standards in Africa is considered.

4.1. AU data protection Convention 2014 (the 'Malabo Convention')

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*,[63] at the African Union's Summit in Malabo, Equatorial Guinea. The African Union (AU), which has as its members all 55 African states now that Morocco has joined, was developing since at least 2011 a draft Cyber-security Convention (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.[64]

As of February 2020, only five countries have ratified this treaty (Senegal, Mauritius, Guinea (Conakry), Ghana and Namibia) and thirteen more countries have signed but not ratified (Benin, Chad, Comoros, Congo-Brazzaville, Guinea-Bissau, Mauritania, Mozambique, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia and Zambia).[65] Six countries without laws have signed (Comoros, Guinea-Bissau, Mozambique, Sierra Leone, Rwanda, and Zambia), and one without either a law or Bill (Namibia) has ratified. Fifteen ratifications are required for the Convention to enter into force (art. 36), so the current eighteen signatures/ratifications indicates that it is feasible that the Convention may enter into force. This is particularly so as

---

effective enforcement needs to be demonstrated, and this requires not only a law on paper but one that is shown over time to be effective in practice. Gayrel of CRID also published a brief analysis of the laws of Tunisia and Morocco, giving more detail of the weaknesses of the (then) Tunisian law, particularly in relation to the public sector (Claire Gayrel 'Data Protection in the Arab Spring: Tunisia and Morocco' (2012) 115 *Privacy Laws & Business International Report*, 18-22).

[62] General Data Protection Regulation (EU) 2016/679 (GDPR)

[63] African Union Convention on Cyber-security and Personal Data Protection (27 July 2014) < https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection >

[64] The AU Convention as many potential state parties than any other international data protection agreement currently has ratifications. Council of Europe Convention 108 has 55 ratifications (see above)

[65] A Status List for this Convention has been published by the AU with the Convention (address above), 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.

the majority of African countries with data privacy laws (17/31) have as yet neither signed nor ratified the Convention. The effect of inclusion of both cyber-security and data protection in the Convention, compared with a convention solely concerning data protection, is uncertain. Lack of resources from the AU to promote ratifications may also have had an effect.

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

Article 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', 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, but are included in the SADC model law. '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 parents (biological or civil) 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), but derived from data privacy principles, 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 (that is, opt-in). There are exceptions 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. 4). There is little coordination between these provisions and those giving a more general right to object to processing (Art. 18(2)).

Enforcement structure and processing formalities

The Convention requires the members States to establish an independent national data protection authority (DPA) which tasks are primarily to monitor and enforce compliance with the data protection legislation, to receive complaints from data subjects and to sanction offenders. Composition and rules of procedure of the DPA are matters to be regulated by the member States independently, according to their respective administrative standards. Consequently the Convention does not impose any model of organization of the DPA; members States are free to opt for a commission or a commissioner, and free also to decide for an authority exclusively dedicated to data protection or an authority dealing with other issues like cybersecurity or transparency and access to information. Whatever solution is chosen, the DPA has to be provided with sufficient human and financial resources to perform efficiently its tasks (art. 11.3).

The framers of the Convention were keen to safeguard the independence of the DPA. Thus the Convention expressly forbids any public authority to give instructions to the DPA or to its members. Likewise members of the Government as well as executives or shareholders of companies operating in the information and communications sectors cannot be appointed to the DPA. Lastly, members of the Commission enjoy full immunity for opinions expressed in pursuit of their duties. One can however regret that the Convention does not restrict the grounds for dismissing members of the DPA; this silence leaves the door open for retaliation against members deemed too interventionist. (Art. 11. 6-8).

The DPA must have broad powers to impose remedies and sanctions to contraventions to the national data protection legislation, including (subject to appeals in all cases) powers to investigate, to give warnings, to discontinue or block processing where fundamental rights are threatened, to inform judicial authorities of offences and to impose monetary fines, (art. 12).

The involvement of DPAs in personal data processing should not be limited to ex-post interventions following complaints of data subjects or own motion inquiries. According to the Convention, the DPAs are to be associated at the earliest stage of processing. Thus, most processing is subject to preliminary formalities, of which there are 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)).

Education of stakeholders in matters of data protection and development of industry code of conducts are tasks not addressed by the Convention. The Guidelines fill the lacuna by strongly recommending that DPAs engage in these preventive activities.

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 in the European Union's data protection Directive (at that time, and now in the GDPR). 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[66]) 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,[67] 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. For example, Chad (art. 29) requires free data flows between members states of ECCAS and CEMAC, but not to other countries. 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 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 the Council of Europe's Convention 108 (and now 108+), it does not require reciprocal 'free flow' of personal data between parties to the AU 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.

Personal Data Protection Guidelines for Africa (2018)

The Convention has been complemented by *Personal Data Protection Guidelines for Africa* issued in May 2018.[68] Created by the Commission of the African Union with considerable support of the Internet Society and privacy experts from Africa, this text aims at facilitating the implementation of the Convention, and draws inspiration from other international data protection instruments, which it finds to be largely consistent.[69] Though far from being an

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

[67] 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.

[68] Internet Society and Commission of the African Union *Personal Data Protection Guidelines for Africa*, 9 May 2018 https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/ ('AU Guidelines').

[69] The authors of the Guidelines expressly acknowledge the revised (2013) OECD Privacy Guidelines, the 108 Council of Europe Convention on Data Protection and the updated (2015) Asian-Pacific-Economic Cooperation Privacy Framework and, more broadly, the EU General Data Protection Regulation of 2016 as providing the foundations of privacy policies and practices.

authoritative commentary or an explanatory report of the Convention text, the Guidelines might offer some help when it comes to interpret unclear or vague requirements of the Convention. However, the Guidelines are designed as recommendations and thus are of non-binding nature.

To a certain extent the Guidelines also update informally the Convention, as they envisage new principles like data minimization (and the avoidance of unmanageable risks), privacy by design, accountability of data controllers, codes of conduct and certification. The Guidelines recommend greater consistency in national data privacy laws in African, particular in relation to establishment of data protection authorities, enforcement measures, and 'common and consistent criteria for assessing adequacy' to 'enable cross-border transfers in the AU'.[70]

The Guidelines recommend the establishment, under the auspices of the AU, of an 'Africa-wide personal data protection committee', a multi-stakeholder expert body to advise the AU on a wide range of issues, but particularly on how to build up certification systems.[71]

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 tools. 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' is considered in the following section.

4.2. Other Africa-wide agreements and declarations

African human rights conventions and courts, free trade agreements, and civil society declarations are also relevant to the protection of privacy in the continent.

African human rights conventions and courts

Created in 1981, the African Charter on Human and Peoples' Rights (ACHPR or 'Banjul Charter')) lays down minimal standards and freedoms for the promotion and protection of human rights in Africa.[72] It has been signed and ratified by all African states except South-Sudan. Though modeled on equivalent international or regional instruments, like the International Covenant on Civil and Political Rights or the European Convention on Human Rights, the African Charter does not explicitly protect the right to privacy, or to private life. However, various clauses provide that human beings 'are inviolable', 'entitled to respect for his life and the integrity of his person', 'the respect of the dignity inherent in a human being', and 'the right to liberty and to the security of his person', as well as not to be 'arbitrarily deprived' of these rights.[73] Similar terms have been found to provide an implied right to privacy in national constitutions. The nevertheless regrettable omission of express protection has been partially filled by the African Charter on the Rights and Welfare of the Child (1990) which expressly protects privacy of infants (art. 10).

---

[70] AU Guidelines, p. 19.

[71] AU Guidelines, ppp. 21-2.

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

[73] ACHPR, arts. 4-6.

In order to ensure implementation of the rights enshrined under the Charter (ACHPR), an African Commission on Human and Peoples' Rights has been established (see Part II of the Charter). This supranational organism has been vested with powers to monitor member states (periodical reviews) and to receive complaints submitted by individuals or NGOs (communication procedure). The Commission delivers general resolutions on human rights issues as well as binding decisions. As the Charter does not expressly protect privacy, the Commission has no competence to deal directly with privacy issues; nonetheless, it has often underscored, in broad terms, the importance of adequate privacy protection.[74]

In 2006 an African Human Rights Court (AHRC) was established with the aim of creating a fully fledged judicial dispute resolution mechanism[75]. Only ten States (Benin, Burkina Faso, Côte d'Ivoire, Gambia, Ghana, Malawi, Mali, Rwanda, Tanzania, and Tunisia) have made the declaration recognizing the competence of the Court to receive cases from NGOs and individuals. All except Rwanda, Gambia and Tanzania have data privacy laws. Tanzania has now withdrawn its declaration. [76]

African Continental Free Trade Area agreement (AfCFTA)

In other parts of the world, free trade agreements (such as the CPTPP in the Asia-Pacific) have included clauses which impose more strict restrictions on personal data export limitations in national laws, than are imposed by the global standard, the WTO's General Agreement on Trade in Services (GATS), art. XIV(c)(ii).[77] They also include very strict conditions on data localisation provisions.

The African *Continental Free Trade Area* (AfCFTA)[78] is a continent-wide African Union (AU) free-trade agreement signed by 49 (of 55) AU member states by April 2019,[79] after being open for signature in Kigali, Rwanda on March 21, 2018. As of April 2019, it has been ratified by the required 22 signatories, and came into force on 30 May 2019, and is operational since a summit in July 2019.[80] It will result in the largest free-trade area in terms of participating countries since the formation of the World Trade Organization. [81] Article 15 'General Exceptions' of the Agreement[82] provides in art. 15(c)(ii) protection, in terms indistinguishable from that in the GATS, to measures which are not unjustifiable discriminatory between state parties, and are relating to 'the protection of the privacy of individuals in relation to the

---

[74] See among others the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX) 2016, and the General Comments on Article 14 (1) (d) and (e) of the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa where the Commission stated that the right to self protection established by art. 14 includes the right to privacy.

[75] See the 1999 Protocol to the ACHPR on the Establishment of an African Court on Human and Peoples' Rights. As yet 30 States have ratified this protocol.

[76] Nicole de Silva 'Individual and NGO Access to the African Court on Human and Peoples' Rights: The Latest Blow from Tanzania' *EJIL: Talk!* 16 December 2019 < https://www.ejiltalk.org/individual-and-ngo-access-to-the-african-court-on-human-and-peoples-rights-the-latest-blow-from-tanzania/>.

[77] Greenleaf, G. 'Looming free trade agreements pose threats to privacy' (2018) 152 *Privacy Laws & Business International Report* 23-27 <https://papers.ssrn.com/abstract_id=3199889>

[78] About CFTA - Continental Free Trade Area (website) < https://au.int/en/ti/cfta/about>; see also Wikipedia: African Continental Free Trade Area.

[79] The non-signatories are Benin, Botswana, Eritrea, Guinea-Bissau, Nigeria, and Zambia.

[80] Shoshana Kede 'Africa free trade agreement gets last ratification from Gambia' *African Business*, 2 April 2019 <https://africanbusinessmagazine.com/uncategorised/continental/africa-free-trade-agreement-gets-last-ratification-from-gambia/>. See also < https://en.wikipedia.org/wiki/African_Continental_Free_Trade_Area> for current status..

[81] Justina Crabtree, CNBC, 20 Mar 2018): "Africa is on the verge of forming the largest free trade area since the World Trade Organization"..

[82] 'Agreement Establishing The African Continental Free Trade Area' <https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area>.

processing and dissemination of personal data'. [83] It is therefore unlikely that conventional data export limitations (such as requirements of 'adequate' or 'comparable' protections) in national legislation in African states will be open to successful attack by other states.

Civil society's Africa-wide Internet Declaration

In 2014, only a few weeks after the AU Convention's 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*.[84] Two of the Declaration's twelve 'Key Principles' are demands for protections on the Internet of privacy (including personal data), and data security.[85] The Declaration also includes strong statements against mass surveillance.[86]

Each key principle is supplemented by application standards which detail the necessary measures to be taken. Regarding data protection in particular, conformity with the fundamental data processing principles (fairness, purpose specification, accuracy and transparency) is required; the Declaration also expressly calls for the establishment of data breach notification mechanisms.

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 call for data privacy protection in Africa is therefore now coming from both government and civil society alike, though with different emphases.

4.3. Cooperation between African data protection authorities (DPAs)

The Convention makes it a goal of African DPAs to set up cooperation mechanisms among themselves and with other DPAs (Art. 12. 2(m)). Consequently, an organisation linking the DPAs in African countries, the African DPA Network (Réseau Africain des Autorités de Protection des Données Personnelles or RAPDP),[87] was created in September 2016, on the margins of the francophone AFAPDP[88] conference, by adoption of its statute in Ouagadougou

[83] CFTA art. 15(c)(ii) 'Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between State Parties where like conditions prevail, or a disguised restriction on trade in services, nothing in this Protocol shall be construed to prevent the adoption or enforcement by any State Party of measures: … (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Protocol including those relating to: … ii. the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts…'

[84] 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>.

[85] '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.'

[86] '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.'

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

[88] The 'Association francophone des autorités de protection des données personnelles' (AFAPDP) <https://www.afapdp.org>, founded in 2007, has as members 27 data protection authorities of 24 countries that are members of the 'Organisation Internationale de la Francophonie' (OIF).

(Burkina Faso), subsequently amended in Morocco in 2018. According to its articles of association (art. 5)[89], the aim of the network is to create an institutional framework to share privacy practices, to support the implementation of national data protection legislations and to foster mutual cooperation between African DPAs. The eleven members of the Network (Benin, Burkina Faso, Cape Verde, Ghana, Ivory Coast, Mali, Morocco, Senegal, South Africa, Sao Tome & Principe and Tunisia[90]) met in 2018 on the side of an international conference of DPAs organised by Morocco's DPA.[91] Discussions there focused on reinforcing the voice of Africa within the different international organizations dealing with data privacy, such as but not exclusively the ICDPPC (now GPA). The first separate RAPDP conference (General Assembly) took place in Accra, Ghana in June 2019.

Given that ten African countries have not yet appointed the DPAs for which their laws provide, that means there are another ten DPAs who could be members of RAPDP, but are not. The success of RAPDP, and perhaps of the development of data privacy in Africa, may depend to a large extent on whether RAPDP can obtain the active involvement of most African DPAs (not only one third of its potential membership as at present), so as to provide mutual support, training and development of standards. One disadvantage, compared with the GDPR's European Data Protection Board (EDPB) or the Convention Committee of Convention 108, is that RAPDP does not have any formal role under the AU Convention, and will have to create its own.

5. African regional data privacy instruments and the RECs

African countries started to adopt data protection laws because of mainly national preoccupations, including the growing use of computers to manage State activities such as issuing identification documents (Burkina Faso 2004) or electoral lists (Benin 2009), and the growing operation of private outsourcing activities from European countries (Mauritius and Tunisia 2004; Senegal 2008; Morocco 2009). In some countries there were also strong human rights concerns.[92] More recent legislation has been justified by the need to create trust for customers and legal certainty for foreign companies operating in Africa. There is an increasing ambition to be EU compatible (Benin, Tunisia, Mauritius). 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.

This section focuses on regional developments, and the important data privacy agreements and model laws in sub-regions or Regional Economic Communities (RECs) of Africa.[93] Africa has at least eight RECs,[94] 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

[89] RAPDP articles of association <http://cnilbenin.bj/statut/>. So far this constitution is available only in French (though Arabic, English and Spanish are also official languages of the Network).

[90] Full membership to the network is limited to countries which already have appointed DPA; countries which have adopted national data protection law (or who are in the process of adopting such a law) are granted observer status (art. 6 articles of association). Membership as of 2019 is at < https://apdp.bj/evenements/assemblee-generale-du-reseau-africain-des-autorites-de-protection-des-donnees-personnelles/>.

[91] *International Conference on the protection of private life and personal data in Africa* <https://www.coe.int/en/web/data-protection/-/international-conference-on-the-protection-of-private-life-and-personal-data-in-africa.>

[92] Lo p. XXX

[93] 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>.

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

purpose of these sub-regional developments is now outlined, focusing on their influences and history.

5.1. 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 states[95] 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)[96] 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.[97] The ECOWAS Supplementary Act was a project assisted by the EU/ITU in 2005-7, as a precursor to the broader HIPSSA initiative. All requirements are influenced very strongly by the EU data protection Directive of 1995 as developed in the data protection law of Senegal.

In 2011 the Supplementary Act was complemented by the Directive C. Dir. 1/08/11 on fighting cybercrime within ECOWAS which, among others, criminalizes violations of the principles and formalities governing process of personal data laid down by the Supplementary Act[98].

Standards contained in the ECOWAS Supplementary Act

The AU Convention is very similar to the ECOWAS Act. That is not at all a matter of coincidence; the framers of the AU Convention drew their inspiration from the four years older ECOWAS Act[99]. Thus, structure, scope and content do not differ (though the wording of some provisions might not always be the same[100]). In particular both texts envisage formalities of DPA notification/authorization of data processing with (comparable) exceptions. They also establish similar data processing principles as well as similar rights for the data subject and similar obligations for the data controller. In addition, the ECOWAS Act and the AU Convention require the establishment of an independent national data protection authority, the tasks and powers of which are framed identically.

Among the very few differences, it should be noted that the ECOWAS Act exempts any domestic processing of personal data whereas the AU Convention restricts the exemption to data which are not systematically communicated to third parties.[101] On the other hand, the ECOWAS Act is also applicable to temporary technical activities, like caches (contrary to art. 4 AU Conv). Another major difference is to be found in the list of data protection principles:

---

[95] 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. Mauritania who left ECOWAS in 2000 is now back as an associate member.

[96] Supplementary Act on Personal Data Protection within ECOWAS <http://www.statewatch.org/news/2013/mar/***ecowas***-dp-***act***.pdf >

[97] So far, no case of data protection has been submitted to the ECOWAS Court.

[98] See in particular art. 12 "Fraudulent manipulation of personal data".

[99] Lo, p. 52.

[100] Compare for example the wording of art. 43 ECOWAS *The data controller shall take all necessary precautions in relation to the nature of data, and in particular to ensure that it is not deformed, damaged or accessible to unauthorised third parties*, with the wording of the parallel provision of the AU Convention (art. 21) *The data controller must take all appropriate precautions according to the nature of the data, and, in particular, preventing it from being altered or destroyed, or accessed by unauthorized third parties.*

[101] This may be influenced by the CJEU decision in *Lindqvist* CLI:EU:C:2003:596.

according to art. 13 AU Conv data processed should be adequate, relevant and *not excessive*. The latter requisite is missing in ECOWAS.

Laws enacted in ECOWAS states

Eleven of the fifteen ECOWAS states have enacted laws (Benin, Burkina Faso, Cape Verde, Senegal, Ghana, Guinea, Ivory Coast, Mali, Niger, Nigeria and Togo), although four of these (Cape Verde, Burkina Faso, Senegal and Benin) predated the 2010 ECOWAS Act and influenced its provisions. The last three of these were in turn influenced by France's law. Quite often the provisions of the later laws are directly drawn from the Supplementary Act. Guinea, Mali, Niger and Togo are emblematic in that respect: the rules on mandatory declaration of data processing, on authorization for sensitive data files, on the right of access as well as the principles guiding processing of personal data are merely copied and pasted provisions of the Supplementary Act.

Four ECOWAS members are yet to enact legislation or propose Bills since the 2011 Supplementary Act (Gambia, Guinea Bissau, Liberia, and Sierra Leone). It is a matter of dispute whether the Supplementary Act is directly applicable and legally binding without enacting legislation, and thus already offers protection to the data subjects in these six countries. In the absence of any jurisprudence of the ECOWAS Court regarding the legal nature of ECOWAS supplementary acts in general, this question remains a matter of controversy. Three positions are possible. Some scholars, referring to the doctrine of supremacy of EU secondary legislation, consider supplementary acts as intrinsically superior to domestic laws, and thus directly applicable with the consequence that the rights and obligations which they enshrine are immediately enforceable.[102] Others scholars deny supranational character (direct application) to the supplementary acts; accordingly, prior domestic incorporation would be a requisite for enforceability, at least in the so called dualist states (being common law countries, with Liberia and Nigeria undoubtedly belonging to that category).[103] We suggest that a third position, which avoids taking sides in this doctrinal dispute, can be based on art. 48 of the Supplementary Act, which states that national applicability requires its publication in the respective Official Journal of the Member State. At least 6 member States have complied with this formality (Benin, Burkina Faso, Cape-Verde, Ghana, Niger and Senegal), all of which have enacted legislation. It is arguable that the four states with no legislation are not directly bound by the Supplementary Act because none have published it in their Official Journal.

5.2. 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).[104] 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

[102] Most recently Lo, p 51 and Julien C. Hounkpe, Décryptage de la Loi portant Code du numérique du Bénin, CIO Mag, February 2018. The ECOWAS Commission seems also to be of the opinion that supplementary acts are directly applicable, see <http://www.ecowas.int/ecowas-law/find-legislation/>. We understand that ECOWAS takes this position.

[103] Jerry Ukaigwe, *ECOWAS Law* (Springer 2016), p. 211-2017.

[104] 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>

legislations in sub-Saharan Africa.'[105] HIPPSA 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 HIPPSA 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'),[106] which is also relevant to the EAC, and to ECCAS. These Model Laws are more elaborate and to a certain extent more progressive than the ECOWAS Supplementary Act and the African Union Convention. Thus the differences are not just a matter of wording but also of substance and of precision. Very often the provisions of the Model laws go into more practical details, such as delineating in concrete terms the role of the data processor or defining a comprehensive regime of processing personal data for scientific research.[107] These significant differences may be explained on one hand by the fact that a model law, like a recommendation, is not binding. As a result, representatives of the framer states (in most cases the Ministers of telecommunication) feel less committed and are more keen to accept more compelling standards. On the other hand the Model laws, which have been framed in cooperation with European experts, have undoubtedly been strongly influenced by innovative views which were reflected in the first drafts of the EU GDPR.

Southern Africa (SADC)

The Southern African Development Community (SADC) encompasses 15 countries[108] in southern and central Africa, and Indian Ocean states, seven of which have data protection laws (Angola, Lesotho, Madagascar, Mauritius, Seychelles, and South Africa – and Zimbabwe only for its public sector), and three of which have current Bills (Zambia, Tanzania and Swaziland). There has already been work done on SADC-wide data protection laws and policies[109], and the *SADC Model Law on Data Protection*[110] is part of the EU/ITU HIPSSA project.

Once it comes into full effect, South Africa's law may be a significant stimulus to adoption of laws in at least the other SADC countries because of South Africa's role as the regional economic power. However, despite the appointment of its Information Regulator, most provisions of South Africa's 2013 legislation are still not in force. The extent to which the South African law, and other laws in the SADC region, are influenced by the SADC Model Law will be examined in the next article.

---

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

[106] 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>

[107] Other examples of more precise framing of provisions are to be found at 15 SADC (withdrawing the consent to processing of sensitive data (art.), at art. 24 SADC (security measures to be taken by the data controlle) , at art. 45 SADC (fixed deadline to comply with a request of access.

[108] 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/>.

[109] 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.

[110] *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>

East Africa (EAC)

Less advanced in data protection developments until recently is the East African Community (EAC), a regional group of six East African countries (Kenya, Tanzania, Uganda, South Sudan, Rwanda and Burundi)[111], where English and French are variously spoken. In 2019 both Uganda and Kenya enacted data protection laws, with Kenya's law being somewhat stronger than that of Uganda, but both heavily GDPR-influenced. [112] Tanzania and Zambia also have Bills.

EAC has encouraged member states to adopt data privacy legislation.[113] Such initiatives include the adoption in 2012 by the EAC legislature of a *Bill of Rights for the East African Community,* which (unlike the African Charter on Human and Peoples' Rights) incorporates an explicit right to privacy (art. 19). This instrument in not yet in force as it is still awaiting assent of the EAC Heads of State. 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 II[114] 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.[115] The EU/ITU 2012 'Model-law on data protection' was also aimed at the EAC countries, but EAC has not adopted its own version, unlike SADC or ECCAS/CEMAC.

Central Africa (ECCAS and CEMAC)

The Economic Community of Central African States (ECCAS) has eleven member states,[116] which are primarily French and Portuguese-speaking. The Communauté économique et monétaire de l'Afrique centrale (CEMAC) has six French speaking member states that are also members of the ECCAS.[117] Of the ECCAS countries seven of eleven (Angola, Chad, Guinea, Gabon, Equatorial Guinea, Sao Tome & Principe and Congo-Brazzaville) have enacted data privacy laws. None of the other member states are known to have Bills undergoing enactment.

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 (art. 6 and 7), while in the SADC model law developments are made on processing of medical data related to sexual life for research purposes.[118] In

---

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

[112] See Greenleaf and Cottier '2020 ends a decade of 62 new data privacy laws'.

[113] 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(1) *Computer Law and Security Review* 78-89.

[114] 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>.

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

[116] The member countries of ECCAS, founded in 1983, are: Angola, Burundi, Cameroon, Congo-Brazzaville, Democratic Republic of Congo, Gabon, Equatorial Guinea, Chad, Rwanda and Sao Tome and Principe: see ECCAS <http://www.ceeac-eccas.org. The CEMAC member states are Cameroon, Central African Republic, Chad, Congo, Equatorial Guinea, and Gabon <https://www.cemac.int>.

[117] Cameroon, Equatorial Guinea, Central African Republic, Congo-Brazzaville, Gabon, and Chad

[118] 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>.

addition the CEMAC draft directive expressly provides for civil compensation in case of illegal process of data (art. 39).

The innovative content of the HIPSSA model laws

As mentioned above, the HIPSSA model laws are more developed than the ECOWAS Supplementary Act and AU Convention. The major innovations introduced by the Model laws are (as a matter of simplification reference is made to the provisions of SADC) :

1. A wider territorial scope of applicability as the model laws encompass also 'the processing of personal data by a controller who is not permanently established on [given country] territory, if the means used, which can be automatic or other means is located in [given country] territory'. In this case a local representative has to be appointed (art. 2 SADC).
2. A pluralistic composition of the DPA (in particular judges, members of the parliament and representative of civil society organization), and very limited possibilities of removal of the members of the DPA (art. 3 SADC).
3. Regulatory powers of the DPA are subject to veto right of the Parliament (art. 4d SADC; such veto right in not mentioned by CEMAC)
4. A specific legal regime for the process of genetic, biometric and health related data (art. 16 SADC).
5. A right to know whether compliance with a request for information is compulsory or not, as well as what the consequences of the failure to comply are (art. 21 SADC).
6. Specific information duty in case data is collected from third parties (art. 22 SADC).
7. Data breach notification rules (art. 25 SADC).
8. Obligation for the data controller to demonstrate compliance with data protection rules (art. 30 SADC).
9. Information about the basic logic involved in automatic processing of data be should be provided to the data subject in case of automated decision making (art. 31 SADC).
10. Notification to third parties of any modifications to data pursuant to the right of access (art. 32 SADC).
11. Effective assistance to the data subject in case of judicial appeal (art. 40).
12. A detailed regime for export of data, modelled on the EU regime (however no free flow of data between states adopting the SADC model law) (art. 43-45).

5.3. North Africa

North Africa (north of the Sahara) does not have a sub-regional institution with an active interest in data privacy,[119] and proposed northward expansion of ECOWAS has stalled.[120] Tunisia (2004) and Morocco (2009) already have data privacy laws, active DPAs, and have acceded to Convention 108. From 2018 there has been vigorous debate in Tunisia on replacing its authoritarian-era law, adopted before the 'Spring revolution', with one more

[119]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>.

[120] Morocco and Tunisia have applied for membership in ECOWAS, but no final decision have been taken. Some member states, in particular Ivory Coast, are not eager to accept two countries where unemployment rates are higher than in sub-Saharan Africa.

suited to a democratic regime and GDPR influences.[121] Algeria enacted a data protection law in 2018, but it has not yet been promulgated, and does not include an independent DPA.

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, for exchange of views, capacity building cooperation and an influence for consistency. Its current chair is the Tunisian Commissioner, who is also the current chair of the RAPDP (see part 4.3).

The relative lack of independence of data protection authorities, at least in formal legislation if not in practice, has been more common in these North African countries than elsewhere in Africa. Morocco's accession to Convention 108 was delayed, in part because of this issue, and its law is now being revised. The Tunisian Law is also being revised, in particular to strengthen the independence of the DPA and the control over public sector personal data processing.

The second article in this series will consider how similar the Acts and Bills in North African states are to those elsewhere in Africa, despite the lack of a regional standard.

6. The evolution of European and African multinational standards

The three African standards (ECOWAS 2010; SADC 2013; and AU Convention 2014), discussed in this and the two following sections, were all developed subsequent to the initial two European multinational instruments (Council of Europe Convention 108, 1981, plus Additional Protocol 2001, and European Union data protection Directive, 1995), and were influenced by those European instruments. Since those African standards were developed, there have been two new European instruments which have global implications: the EU's General Data Protection Regulation (GDPR, 2016 – in force May 2018), and the Council of Europe's revised 'Convention 108+' (open for signature since October 2018). In practice, these influences were often indirect, via the transpositions of the Directive (and implementations of the Convention) into the national languages of laws of European states, which are the shared languages of their former colonies. African experts brought these influences and knowledge to the negotiation of African multinational instruments.

6.1. Comparison of European and African instruments

To aid comparisons made throughout the rest of this article, the following four Tables set out features of those four European and three African instruments in chronological order (from left to right), for purposes of comparison. This Table enables comparisons to be made such as the extent to which: (i) the three African instruments have similar features; and (ii) the three African instruments have features anticipated by the preceding European instruments; and (iii) the three African instruments include some elements now present in the two recent European instruments. These questions are address in the following sections. The extent to which the content of both the African and European instruments are reflected in the existing national African laws is addressed in the next article.

The Tables classify each of the principles (or standards) identified as being 1st, 2nd, or 3rd 'generation' principles, according to where the first appeared in the European or international instruments under consideration. '1st generation' refers those standards which are common to Convention 108 of 1981 and the OECD privacy Guidelines of 1980. '2nd Generation' refers to

[121] Emna Sayadi 'In Tunisia, an open debate on data protection and the right to access information' *Access Now website*, 8 November 2018 <https://www.accessnow.org/in-tunisia-an-open-debate-on-data-protection-and-the-right-to-access-information/>

the EU dat protection Directive of 1995 (DPD) and the Amending Protocol to Convention 108 of 2001. '3rd Generation' refers to the additional standards found in the EU GDPR of 2016 and to a lesser extent in Convention 108+ of 2018. The 3rd Generation principles are divided into those common to both the GDPR and Convention 108+, and those which are only found in the GDPR but not in Convention 108+, thus providing four Tables. This approach to analysis via 'generations' of data privacy principles, has been more fully explained and utilised elsewhere.[122]

The conventions used in these Tables are generally self-explanatory, but to clarify: C108 = Convention 108; &AP = Additional protocol of 2001 to Convention 108; C108+ = 'modified' Convention 108 of 2018; DPD = EU Data Protection Directive of 1995; GDPR = EU General Data Protection Regulation of 2016. A dash (–) indicates the absence of the standard from that instrument.

Table 1: 1st Generation standards (1981-) implemented in Africa

I	1st Generation standards	Conv. 108 1981	ECOWAS 2010	SADC Model 2013	AU Conv. 2014	GDPR 2016
1.01	*Collection* – limited (not excessive), lawful (for legitimate purposes) and by fair means[123]	C108 5(a), (c)	24	12	–	GDPR 5(1)(a)
1.02	*Data quality* – relevant, accurate, up-to-date	C108 5(c)(d)	26	11(1)	13(4)	GDPR 5(1)(d)
1.03	*Purpose specification* by time of collection	C108 5(b)	25(1)	13	–	GDPR 5(1)(b)
1.04	*Notice of purpose/rights* [assumed implied, but not explicit until EU Directive[124]]	C108 5(b) **C108+ 8**	**–**	**21(1)**	**15**	**DPD 10,11** GDPR 13, 14
1.05	*Uses limited* (including disclosures) to purposes specified or compatible	C108 5(b)	25(1)	13(1)	13(3)(a)	GDPR 5(1)(b)
1.06	*Security* through reasonable safeguards	C108 7	28; 43	24	13(6);20; 21	GDPR 5(1)(f), 32
1.07	*Openness* re personal data practices (not limited to data subjects)	C108 8(a)	–	–	–	GDPR 14(5)(b)[125]
1.08	*Access* – individual right of access	C108 8(b)	39	31	17	GDPR 15
1.09	*Correction* – individual right of *correction* [126]	C108 8(c), (d)	41	32	19	GDPR 16, 19
1.10	*Accountable* – identified data controller accountable for	C108 8	42	–	–	GDPR

[122] Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 53-58. However, this discussion pre-dates the '3rd Generation' standards., although the idea of three generations is workable enough for this context.

[123] OECD Guidelines 1980 add 'with consent or knowledge'; CoE 108 does not until C108+ 5(2) in 2018.

[124] Both EOCD and C108 imply some notification should be given of purpose of collection, but do not require it at time of collection. OECD 9 EM [54] leaves method and timing optional; C108 5(b) EM says use of 'specified' leaves option to Parties to require notice, and when it is required (see EM); Explicit notice to data subject is only required by EU DPD 10 (for collection from data subject at time of collection), and 11 (for collection from 3rd P, at time of recording/disclosure); C108+ 8 adds notice required at time of collection, and usually required when collected from 3rd party.

[125] A more limited obligation, applying only where individual notice is not given.

[126] Notice to 3rd parties only explicit in EU DPD; EU DPD 12(c) required notice of corrections/ blocking to be sent to 3rd P recipients; GDPR 19 does likewise; Conv 108+ 9 does not.

	implementation	5(1)(f)

Table 1 shows that the three African instruments require, on average, that national laws in Africa should include 8/10 of the '1st generation' requirements found in Convention 108 and the OECD Guidelines,[127] including the essential standards of individual access and correction rights, security, and 'finality' (purpose limitation requirements).

Although the focus of Table 1 is the standards found in Convention 108 as at 1981, it also indicates where these ten 'first generation' standards appear in the later European instruments.

Table 2: 2nd Generation data privacy standards (1995–) implemented in Africa

II	2nd Generation – 'European standards' – post-1995	EU DPD 1995	Conv 108 & AP 2001	ECOWAS 2010	SADC 2013	AU 2014	GDPR 2016
2.01	*Minimum collection* necessary for the purpose (not only 'limited') (data minimisation)[128]	6(1)(b),(c), 7	**C108 5(c);** C108+ 5(4)(c)[129]	–	–	10(3)(b)	GDPR 5(1)(c)
2.02	*Destruction or anonymisation of personal data after purpose completed*[130]	6(1)(e)	**C108 5(e);** C108+ 5(4)(e)[131]	41	32(1)(b)	22	GDPR 5(1)(e)
2.03	*Additional protections for sensitive data* in defined categories	8	C108 6	30	15	1def; 14	GDPR 9, 10
2.04	*Legitimate bases for processing defined* [Weaker: general requirement of 'fair and lawful processing' (not only collection)]	7 [6(1)(a)]	*– C108;* ***C108+ 5(2);*** [C108 5(3), (4)(a) [132]]	25	12, 14	1def; 13(1),(2)	GDPR 6 [GDPR 5(1)(a)]
2.05	*Additional restrictions on some sensitive processing systems* (notification; 'prior checking'[133] by DPA etc)	20	*– C108;* ***C108+ 10(2)***	5, 12	26, 28	10(2)-(4)	GDPR 36
2.06	*Limits on automated decision-making* (incl. right	15, 12(a)	*– C108*; ***C108+***	35	31(1c), 36	–	GDPR 22

[127] These ten standards are also found in the OECD privacy Guidelines, but that is not relevant to Africa, since there are no OECD Member countries in Africa. It is not feasible to attempt to distinguish between indirect influences from the OECD Guidelines as against other international instruments that share the same standards.

[128] Both EU Dir and CoE use 'not excessive', but EU Dir adds 'necessary', except for processing with unambiguous consent. C108+ 5(c) retains 'not excessive' but draft EM [52] states this means minimal collection and anonymity where possible. GDPR 1(c) 'data minimisation' says 'limited to what is necessary'.

[129] C108 5(c) uses the term 'not excessive'.

[130] Both EU Dir and C108 technically only require pseudonymisation – see C108 EM – but their wording appears to require anonymisation. GDPR 1(e) 'storage limitation' retains similar wording.

[131] C108 5(c) uses the term 'not excessive'.

[132] C108 has a general requirement of 'fair and lawful processing' (not only collection), but does not (unlike the DPD) define legitimate grounds for processing.

[133] GDPR now refers to 'prior consultation'. C108+ does not require prior consultation of DPAs, leaving this to national law.

	to know processing logic)[134]		***9(1)(a), (c)***				
2.07	*To object to processing on compelling*[135] *legitimate grounds, including to 'opt-out' of direct marketing uses* of personal data[136]	14(a), (b)	– *C108*; ***C108+ 9(1)(d)***	40	33	18	GDPR 21
2.08	*Restricted data exports required* based on data protection provided by recipient country ('adequate'), or alternative guarantees	25, 26	***C108 AP2***; C108+ 14	36	43	14(6)(a)[137]	GDPR 45–47
2.09	*Independent Data Protection Authority(-ies)* (DPA)[138]	28	***C108 AP 1***; C108+ 15	14(2)	3(1)	11(1)(b)	GDPR 51-59, 77
2.10	*Recourse to the courts* to enforce data privacy rights[139]	22, 23	***C108 AP 1(4)***; C108+ 12, 15(9)	–	4(c), 39	–	GDPR 78, 79, 82

It is clear from Table 2 that each of the three African instruments are relatively consistent in requiring that national laws in Africa should implement the standards first required by the EU DPD of 1995. There are differences and omissions, but overall the three African instruments on average match 8/10 of the distinctive principles of the EU DPD. This also meant that they required enactment of almost all of the standards required by Convention 108 (including the Additional Protocol of 2001), relevant to African countries wishing to accede to the Convention.

However, these European standards have now become more strict. The EU has enacted the GDPR, and the Parties to Convention 108 (including its non-European, predominantly African, parties) have adopted the amending protocol to convert it into Convention 108+, with higher standards. These higher standards are reflected in the next two tables, where they are compared with the content of the African instruments.

Table 3: 3rd Generation Common European Data Privacy Standards (GDPR and 108+, 2018–)

IIIA	3rd Generation – Common European Standards	ECOWAS 2010	SADC Model 2013	AU Conv. 2014	GDPR 2016	Conv 108+ 2018
3.01	*Data protection by design and by default*	–	–	–	GDPR 25	C108+ 10(2)-(4)
3.02	*Demonstrable accountability* by	–	30(1)(b)	–	GDPR 5(2)	C108+ 10(1)

[134] Not included in C108 AP, but now added by C108+ 8(a), (c).

[135] The word 'compelling' was deleted in the 2014 draft of C108+.

[136] Not included in C108 AP. C108+ 8(d) adds a rights to objection, but does not single out direct marketing.

[137] But no export limits apply to exports to another AU member state.

[138] A weaker implementation of this principle has often been implemented as 'a separate data protection authority', meaning the enforcement of data protection by one authority, rather than by numerous functional Ministries. Where it is limited to the regulation of the private sector, it can be argued that it is not unusual, as a government regulator can still be independent of private sector bodies.

[139] GDPR includes compensation, and appeals from decisions of DPAs; CoE AP 1(4) only provides for appeals against DPA decisions.

	controllers					
3.03	*Data breach notification to DPA* for serious breaches	–	25	–	GDPR 33	C108+ 7(2)
3.04	*Direct liability for processors* as well as controllers	–	–	–	GDPR 28-31	C108+ 7(1), 10(1)
3.05	*Stronger consent requirements* – including 'unambiguous' and unbundled[140]; special conditions for children's consent	–	1(2), 37	–	GDPR 7, 8	C108+ 5(2)
3.06	*Proportionality required* in all aspects of processing	–	–	–	GDPR *passim*[141]	C108+ 5(1), 10(4)
3.07	*DPAs to make decisions and issue administrative sanctions* incl. fines	19	5(2)	12(2)(h)	GDPR 58(1)	C108+ 12
3.08	*Biometric and genetic data require extra protections*	12	16	104(a), (d)	GDPR 9	C108+ 6(1)
3.09	*Stronger right to erasure* incl. 'to be forgotten' [142]	–	–	19	GDPR 17, 19	C108+ 9(1)(d),(e)
3.10	*DPAs must cooperate with other DPAs in resolving complaints with international elements*[143]	–	–	12(2)(m)	GDPR 50	C108+ 16-21

The SADC Model Law, satisfying five requirements, comes closer to meeting the standards common to both Convention 108+ and the GDPR, than does the AU Convention (4), or ECOWAS Supplementary Act (only 2).

Drafts of the proposed GDPR were available, in increasingly more reliable forms, from 2012 onwards, so these drafts were capable of influencing the content of other instruments being developed outside Europe, although causation is usually difficult to show with any certainty. The ECOWAS Act predates GDPR discussions, and it is not surprising that it anticipated little of the GDPR's content. Of these 10 standards, the 2013 SADC Model Act anticipated five, and the 2014 AU Convention anticipated four (but not the same sub-set).

Table 4: 3rd Generation Additional EU (GDPR) Data Privacy Standards (2016–)

IIIB	3rd Generation –GDPR additional standards, 2018– (not in CoE 108+)	ECOWAS 2010	SADC Model 2013	AU Conv. 2014	GDPR 2016
3.11	*Mandatory Data Protection Impact Assessments (DPIAs) for high risk processing*	–	–	–	GDPR 35, 36
3.12	*Extra-territorial jurisdiction,* where goods or services offered, or behaviour monitored	–	–	–	GDPR 3

[140] CoE 108+ only requires 'unambiguous' consent, not 'unbundling.

[141] GDPR does not explicitly require proportionality in all aspects of processing, but it is required in many articles, and referred to in many recitals: GDPR 6(3), (4), 9(2)(g), (j), 23, 24(1), 35(7)(b), 83(1), (9), 84(1), 90(1); Recitals 4, 19, 49, 50, 73, 129, 151, 156, 170.

[142] Although the 'right to be forgotten' (including de-linking) was held by the CJEU to be implied by the DPD, in the Google Spain decision, it (and the broader concept of erasure) has a much longer history in EU data protection law: see Erdos and Garstka 'The 'Right to be Forgotten' Online within G20 Statutory Data Protection Frameworks'. The GDPR reformulates the right to erasure in an arguably stronger and more explicit form.

[143] GDPR 50 is the only generic requirement for international cooperation. C108+ 16-21 expands on previous CoE 13-16; CoE AP 1(5), but all of these only deal with mutual assistance between parties to Convention 108.

3.13	*Extra-territorial controllers or processors must be represented within jurisdiction* (EU/other)	–	–	2(3)	GDPR 27
3.14	*Right to data portability* (UGC / other)	–	–	23	GDPR 20
3.15	*Mandatory Data Protection Officers (DPOs)* for sensitive processing	–	–	–	GDPR 37-39
3.16	*Data breach notification to data subjects* (if high risk) [144]	–	–	–	GDPR 34
3.17	*Representative actions before DPAs or courts by public interest privacy groups*[145]	–	(40)[146]	–	GDPR 80
3.18	*Maximum admin. fines based on annual turnover,* global or local[147]	–	–	–	GDPR 83(4)-(6)

None of these standards are required by Convention 108+. As Table 4 shows, the three African agreements anticipate very few, hardly any, of these additional requirements of the GDPR. A question which now arises is whether the 16 data privacy laws enacted in African countries since 2014 (when all three African instruments had been completed) will tend to adhere to the limited standards found in those instruments, or will they also enact additional standards found in Tables 3 and 4 above, influenced by the GDPR and Convention 108+? This is examined in the second article in this series.

6.1. Consistency of African data protection instruments

In this section the comparison of the three African instruments, utilising the above Tables and other elements of comparison, is continued.

Binding instruments (ECOWAS and AU agreements)

The binding instruments in the African regional framework of data protection are *coherent*, consisting of two international instruments (ECOWAS Supplementary Act and AU Convention) which are very similar. Although the AU Convention is four years older (and not yet in force), it more or less copies the provisions of the former, rather than building on them. Structure and content are the same (though sometimes wordings differ). In particular both texts envisage a (rather old fashioned and cumbersome) system of DPA notification/authorization of data processing with (similar) exceptions. They also establish similar data processing principles (except that art. 13 principle 3 AU Convention proclaims that processed data should not be 'excessive', a requisite which is not mentioned in ECOWAS) as well as similar rights for the data subject and similar obligations for the data controller. Finally, both of them call for an independent DPA, the tasks and powers of which are identical. The only major substantive difference concerns the scope of the legislation (art. 4 AU Convention excludes temporary technical activities from the scope of the act; in addition domestic use is excluded as long as the data are not disseminated or systematically communicated to third parties). These binding agreements reflect strongly the second generation data protection agreements in Europe, as shown in Table 2.

[144] C108+ only requires notice 'at least to supervisory authorities'.

[145] DPD 28(4) only provided for representation by an association in complaints to DPAs.

[146] SADC Model Law envisages a class action system, which is somewhat different.

[147] GDPR 83(4): up to the higher of 10M euros or 2% of global annual turnover of previous year, for specified breaches; GDPR 83(5), (6): up to the higher of 20M euros or 4% of such turnover, for other specified breaches. Although the GDPR requires global turnover to be assessed, the principle involved could be based on national turnover (with adjustment for percentages). The Australian government has so proposed.

We might have expected the AU Convention to be the 'driver' of data protection in Africa, because of the 'keystone' continental position of the African Union. This could have been similar to how Convention 108 was the initial driver of data protection developments in Europe, at least from 1981-1995. Although the framers of the AU Convention had this ambitious goal in mind (as reflected in the Preamble of the AU Convention), the result as yet disappoints this ambition. Only five countries have ratified the Convention (of 15 required by art. 36), although fourteen more have signed it, and many countries have adopted data protection laws without even mentioning the existence of the AU Convention (in either the preamble of their national laws, or during the 'travaux préparatoires'). The fact that the AU Convention addresses two issues at the same time (privacy protection and the more controversial mechanisms to fight cyber-crime) may have given rise to conflicting policy considerations in some countries, and marginalised the Convention's influence. Nonetheless, things may change if the Convention enters into force and encourages the Commission of the AU to more actively promote data protection and to monitor the implementation of the Convention (art. 32). Finally, it should be stressed that, among the African countries that have already adopted a national DP law, two are not in a position to sign and ratify the Convention: Algeria and Morocco do not yet comply with the (strong) requisite of independence of the DPA.

The African regional framework has one significant lacuna: contrary to its European counterparts, it does not establish any international body dedicated to data protection, like the GDPR's European Data Protection Board (or its predecessor, the Article 29 Data Protection Working Party) or the Consultative Committee of Convention 108. A potential driving force, capable of promoting and monitoring compliance with data protection principles across African jurisdictions, is therefore lacking. Perhaps the African Network of DPAs (RAPDP – see [4.3]) may play some role like this in the future, but without a role recognised formally in the regional instruments, this will be difficult.[148] Its membership does not yet include all African DPAs.

Non-binding instruments (HIPSAA model Bills and AU Guidelines)

When we add to this binding AU and ECOWAS framework the non-binding regional texts, there is less consistency. The different HIPSSA model instruments (SADC, ECCAS-CEMAC) as well as the 2018 *Guidelines on Privacy and Personal Data Protection* of the Africa Union Commission (hereinafter Guidelines) are more modern (in particular the latter text), and display some features of third generation data protection laws (the Guidelines directly refer to the GDPR). In addition the provisions are more detailed (see for instance the provision on withdrawing the consent to processing of sensitive data, art. 15 SADC, or the security measures to be taken by the data controller, art. 24 SADC, or the regime applicable to scientific research, art. 11, 13, 15, 31 SADC). The more progressive character of the non-binding texts is not only due to the fact that they are more recent, but also to the fact that representatives of states are more keen to adopt them as they are mere recommendations deprived of any legal power.

Makulilo's brief analysis of the content of the AU, ECOWAS and SADC initiatives,[149] also finds 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'. Given this

[148] For example, in Asia the influence of the Asia Pacific Privacy Authorities (APPA) has been very limited, because there is no regional data protection agreement, let alone one which gives APPA a role.

[149] Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa', section '3. Harmonisation of data privacy policies'

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'.[150] Writing in 2016, Makulilo concluded that the various regional and sub-regional African privacy agreements had yet to have any significant impact.[151] Fourteen more African laws have been enacted since he wrote, so it is relevant to ask whether the situation has changed.[152]

While we accept 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 increase Africa-wide harmonisation of data protection, and at a relatively high level.

6.2. Goals and influences (European and African)

The political goals of these regional frameworks are many-fold (see in particular the preambles of ECOWAS and AU Conv. as well as the introductory sections of the Guidelines, 'African Context' and 'Policy context'). The following goals are most commonly mentioned: economic development by eliminating obstacles posed by differences of privacy regimes (often linked to African integration); establishing the legal basis for a sustainable data driven economy; strengthening of the African voice on the globe; and, but less emphasized than in Europe, securing respect for human rights, in particular privacy of citizens.

Most striking, the African regional framework does not display any Africa-specific approach to data protection. No traces of the less individualist and more communitarian African culture or human rights discourse are to be found in the texts of these laws (their implementation may be a different matter). In fact, framers of the African frameworks seem to accept, tacitly or expressly (see Guidelines p. 9), the necessity to be consistent with other international texts, in particular European instruments (Convention108 and the successive EU instruments). They all include numerous 'European' elements not required by the OECD privacy 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. Thus the strong European flavour of the African framework. One significant factor is that framers of the ECOWAS Supplementary Act have mostly been representatives of francophone African countries, which in turn drew their inspiration from relevant French law and European instruments (Convention 108 and the DPD).

7. Conclusions

While the general understanding of 'globalisation' is that it means adoption of universal standards, in practice when personal data processing in Africa 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

[150] Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa',section '5. Conclusion'.

[151] Alex Makulilo ''The Future of Data Protection in Africa', pp. 377-8, in Makulilo (Ed) *African Data Privacy Laws* (Springer, 2016).

[152] This will be addressed in our second article.

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 African sub-region to act, echoes the strategy that the EU (comprising half of the European countries) took when it adopted the EU data protection Directive of 1995. From the African Union (AU) level, adopting a regional convention seems also logical while the position at the global level is yet to become clear. When taking into account the universal nature of the data protection principles, including the rights of data subjects, one can expect in the coming years more harmonized data protection practices in different regions 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 conflicts between Europeans and US firms – and their countries – will tomorrow involve similar conflicts between Africans and US firms[153] (and perhaps European firms). It is likely that links will continue to strengthen between those in charge of data protection in African states and the AU, on the one hand, and the Council of Europe's push for 'globalisation' of data protection Convention 108. This may occur formally, as new African parties accede to the Convention, or informally because African States with data protection laws and organisations become Observers on the Convention's Consultative Committee. There is as yet no sign of a United Nations global convention which could overtake such developments.,

It took Europe nearly 40 years since 1981 for them to do so, but by 2017 all 47 Member States of the Council of Europe had ratified Convention 108, enacted data privacy laws, and in 2018 they also agreed to the terms of the 'modernised' Convention 108+. The equivalent developments in Africa cannot be expected to happen overnight, but a comparable continentally comprehensive and relatively uniform adoption of data privacy laws, and progressive strengthening of multi-country agreements, may well result in Africa. The global consequences for the irreversibility of data privacy laws, and (given the history of developments in Africa to date) their global consistency based around a European-influenced model, are very significant.

One significant indicator of whether such a global 'levelling up' is likely is how quickly African countries with data privacy laws, particularly countries with major economic and political weight like South Africa and Nigeria, will accede to and ratify the AU Convention. Second is the extent to which countries which do not yet have such laws start to enact laws which are compatible with or stronger than the Convention.

[153] See for example negotiations by the Moroccan DPA with Facebook <https://www.cndp.ma/fr/presse-et-media/communique-de-presse/617-commpress-20-11-2019.html>

Appendix: African countries with data privacy laws

Jurisdiction	Key Law [0]	From[1]	Latest[2]	Member.[3]	Sec[4]	Agreements[5]	DPA[6]	DPA Assocs[7]

[0] **Key Law column** = name of current key law (Earlier key laws may have had different names)

[1] **From column**: Year = year of original data privacy law enacted, for either private or public sector; might not be year of current law

[2] **Latest column**: Year = year of last significant version of law (amendment or replacement) known; 'NYIF' = not yet in force, where bringing into force is delayed more than two years; 'B(201x)' = current official reform Bill, not yet enacted, and year.

[3] **Member column:** listing means country is a member of regional grouping relevant to data privacy (plus '(A)' for Associate members) – ***AU*** = African Union; ***ECOWAS*** = Economic Community of West African States; ***EAC*** = East African Community; ***SADC*** = Southern African Development Community; ***ECCAS*** = Economic Community of Central African States; ***CEMAC*** = Communauté économique et monétaire de l'Afrique centrale ; ***UKOT*** = UK Overseas Territory

[4] **Sector column:** 'Pri' = covers private sector only; 'Pub' = covers public sector only; both = covers both sectors

[5] **International Agreements column** covers the following agreements between countries, each of which involves legal obligations **No entry means country has taken no action**.

Council of Europe Convention 108 = 108 + one of: (IA) = has been invited to accede to the Convention; (AC)= has acceded to the Convention (RP?)

Council of Europe Convention 108+ (Treaty 223) = CoE 108+ **plus either** (S) = signed or (R) = ratified.

African Union Convention = AUConv **plus either** (S) = signed or (R) = ratified.

ECOWAS Act = country is required to comply with the additional data protection Act to the ECOWAS Treaty, 2010.

UN Int'l Convention on Civil & Political Rights = ICCPR = ratified ICCPR (unless (S) = signed); **+OP** = ratified 1st Optional Protocol; [Not-UN] = not UN member, cannot ratify.

African Human Rights Court -= AHRC = country has declared that individuals and NGOs can commence actions in court.

[6] **DPA column** = DPAs are named **plus** 'Not yet appointed' if not; **or** 'None' = no specialised data protection authority; or 'future DPA law intended'

[7] **DPA Assocs column**: inclusion means 'DPA is a member of' the named association of DPAs/PEAs; except (O) = Observer status only: ***GPA*** = Global Privacy Assembly (previously International Conference of Data Protection and Privacy Commissioners) (**except** '(O)' for Observers status for at least 3 years); ***GPEN*** = Global Privacy Enforcement Network; ***AFAPDP*** = Association of Francophone Data Protection Authorities; ***CTN*** = Common Thread Network (anglophone Commonwealth of Nations); ***RAPDP*** = Réseau African sur la Protection des Données Personnelles (African Personal Data Protection Network) ; ***GCBECA*** = Global Cross Border Enforcement Cooperation Arrangement.; ***GPEN-A*** = GPEN Alert member ; ***RAPDP*** = Réseau African sur la Protection des Données Personnelles (African Personal Data Protection Network); ***CoE108CC*** = Council of Europe Convention 108 Consultative Committee member; **except** (O) = Observer status only

Jurisdiction	Key Law [0]	From[1]	Latest[2]	Member.[3]	Sec[4]	Agreements[5]	DPA[6]	DPA Assocs[7]
Algeria	Loi 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.	2018	2018	AU;	Both	ICCPR + OP	Not yet appointed (Autorite Nationale de Protection des Données à Caractère Personnel)	–
Angola	Lei da Protecção de Dados Pessoais	2011	2011	AU; SADC; ECCAS	Both	ICCPR+OP;	Agência da Protecção de Dados	–
Benin	Code du Numérique	2009	2017	AU; ECOWAS	Both	ICCPR+OP; AUConv(S); AHRC	Commission nationale de l'informatique et des libertés (National Commission for Technology and Freedoms)	GPA; AFAPDP; RAPDP
Botswana	Data Protection Act, 2018	2018	2018	AU; SADC	Both	ICCPR	[Not yet appointed] Information and Data Protection Commission]	–
Burkina Faso	Loi Portant Protection des Données à Caractère Personnel	2004	2004	AU; ECOWAS	Both	ICCPR+OP; AU Conv(S); ECOWAS Act; CoE108(IA); AHRC	Autorité de protection des données à caractère personnel (Data Processing and Liberties Commission)	GPA; AFAPDP; RAPDP; CoE108CC(O)
Cape Verde	Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares	2001	2013	AU; ECOWAS	Both	ICCPR+OP; CoE108(RP); ECOWAS Act	Comissão Nacional de Protecção de Dados (National Commission of Data Protection)	GPA; RAPDP; RedIPD; AFDAP; CoE108CC
Chad	Loi 007/PR/ 2015 portant protection des données personnelles (Law No. 007/PR/ 2015 on the Protection of Personal Data)	2015	2015	AU; ECCAS	Both	ICCPR+OP; AUConv(S); ECOWAS Act	Not yet appointed (Agence nationale de sécurité informatique et de certification électronique - National Agency for Information Security and Electronic Certification)	–
Congo-Brazzaville	Loi 29-2019 portant protection des données à caractère personnel	2019	2019	ECCAS; CEMAC	Both	ICCPR+OP; AU(S)	– [future DPA law intended]	
Cote d'Ivoire	Loi relative à la protection des données à caractère personnel du 19 juin 2013	2013	2013	AU; ECOWAS	Both	ICCPR+OP; AUConv(S); AHRC	Autorité de régulation des télécommunications et des TIC (ARTCI) (Telecommunications and ICT Regulatory Body of Côte d' Ivoire)	GPA; AFAPDP; RAPDP
Egypt	Personal Data Protection Law	2020	2020	AU	Both	ICCPR	Not yet appointed [Personal Data Protection Centre]	–
Equatorial Guinea	Ley da Protección de Datos Personales (Law	2016	2016	AU; ECCAS; CEMAC	Both	ICCPR+OP;	Not yet appointed (Organo Rector de Proteccion de Datos	–

Jurisdiction	Key Law [0]	From[1]	Latest[2]	Member.[3]	Sec[4]	Agreements[5]	DPA[6]	DPA Assocs[7]
	1/2016)						Personales)	
Gabon	Loi 001/2011 relative à la protection des données personnelles	2011	2011	AU; ECCAS; CEMAC	Both	ICCPR;	Commissariat à la protection des données personnelles	AFAPDP; RAPDP; CoE108CC(O)
Ghana	Data Protection Act	2012	2012	AU; ECOWAS	Both	ICCPR+OP; AU Conv(R); ECOWAS Act; AHRC	Data Protection Commission	GPA; CTN; RAPDP; GPEN; CoE108CC(O)
Guinea (Conakry)	Loi L/2016/037/AN relative à la cyber-sécurité et la protection des données à caractère personnel	2016	2016	AU; ECOWAS	Both	ICCPR+OP; AU Conv(R); ECOWAS Act	Not yet appointed (Autorité chargée de la protection des données)	–
Kenya	Data Protection Act, 2019	2019	2019	AU; EAC	Both	ICCPR	Not yet appointed (Data Commissioner)	–
Lesotho	Data Protection Act 2011	2011	2011	AU; SADC	Both	ICCPR+OP;	Data Protection Commission	–
Madagascar	Loi N° 2014–038 Sur la protection des données à caractère personnel	2015	2015	AU;SADC	Both	ICCPR+OP	Not yet appointed (Commission Malagasy sur l'informatique et les Libertés (CMIL))	–
Malawi	Electronic Transactions and Cyber Security Act, 2016	2016	2016	AU; SADC	Both	ICCPR+OP	Malawi Communications Regulatory Authority	–
Mali	Loi no 2013/015 du 21 mai 2013 portant protection des données à caractère personnel	2013	2013	AU; ECOWAS	Both	ICCPR+OP; AUConv(S); ECOWAS Act; AHRC; AHRC	Personal Data Protection Authority (Autorité de Protection de Données à Caractère Personnel)	GPA; RAPDP; AFAPDP
Mauritania	Loi 2017-020 sur la protection des données à caractère personnel	2016	2016	AU; ECOWAS (A)	Both	ICCPR; AU Conv(S); ECOWAS Act	Not yet established (Autorité de protection des données)	–
Mauritius	Data Protection Act	2004	2017	AU; SADC	Both	ICCPR+OP; CoE108(RP); AU Conv(R)	Data Protection Office of Mauritius (Commissariat à la protection des données personnelles)	GPA;; AFAPDP; GPEN; CTN; RAPDP; CoE108CC
Morocco	Loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel	2009	2009	AU	Both	ICCPR; CoE108(RP)	National Commission for the Control and the Protection of Personal Data (CNDP) (Commission nationale de contrôle et de protection des données personnelles)	GPA; AFAPDP; RAPDP; GPEN; CoE108CC
Niger	Loi 2017-28 relative à la protection des données à caractère personnel	2017	2017	AU; ECOWAS	Both	ICCPR+OP; AUConv(S); ECOWAS Act	Not yet appointed (Haute autorité de protection des données personnelles)	–
Nigeria	Nigerian Data Protection	2019	2019	AU;	Both	ICCPR ;	Nigerian Information	–

Jurisdiction	Key Law [0]	From[1]	Latest[2]	Member.[3]	Sec[4]	Agreements[5]	DPA[6]	DPA Assocs[7]
	Regulation 2019		[Bill]	ECOWAS		ECOWAS Act	Technology Development Agency	
São Tomé and Principe	Data Protection Law	2016	2016	AU; ECCAS	Both	CoE108; AUConv(S); ICCPR+OP	Agência Nacional de Proteccão de Dados Pessoais	CoE108CC(O)
Senegal	Loi sur la Protection des données à Caractère Personnel	2008	2008	AU; ECOWAS;	Both	ICCPR+OP; CoE108(RP); ECOWAS Act; AUConv(R)	Commission of Personal Data Protection, CDP (La Commission de Protection de Données Personnelles)	GPA; AFAPDP; RAPDP; CoE108CC
Seychelles	Data Protection Act	2004	2004 NYIF	Au; SADC	Both	ICCPR+OP;	Not yet appointed (Data Commissioner)	CTN(O)
South Africa	Protection of Personal Information Act	2013	2013 NYIF	AU; SADC	Both	ICCPR+OP;	Information Regulator	GPA; RAPDP; CTN
Togo	Loi 2019-014 relative à la protection des données à caractère personnel	2019	2019	AU; ECOWAS	Both	ICCPR + OP; AU(S); ECOWAS Act	Not yet appointed (Instance de protection des données à caractère personnel)	–
Tunisia	Loi portant sur la protection des données à caractère personnel	2004	2004 *B(2018)*	AU	Both	ICCPR+OP; CoE108(RP); CoE108+(S) AHRC	National Personal Data Authority	GPA; AFAPDP; RAPDP; CoE108CC
Uganda	The Data Protection and Privacy Act 2019	2019	2019	AU; EAC	Both	ICCPR + OP; AU(S)	National Information Technology Authority – Uganda	CTN(O)