Africa's Multilateral Legal Framework on Personal Data Security: What Prospects for the Digital Environment?

Rogers Alunge(✉)

LAST-JD Program, CIRSFID, University of Bologna,
Lungo Dora Siena 100A, Turin, Italy
alungerogers@yahoo.com

Abstract. As the African continent continues to embrace technological innovations and corresponding infrastructures like the Internet of Things, certain concerns have been raised as regards the security risks related to critical ICT network infrastructures in the continent, as well as the safeguarding of the fundamental rights of Africans through the protection of their personal data, especially those shared online. One of such concerns is personal data security, which becomes more crucial as huge amounts of sensitive personal data are increasingly generated across the continent, especially with the proliferation of mobile banking. In response to these developments, African intergovernmental organizations have developed legal frameworks on personal data protection: the Economic Community of West African States (ECOWAS) has adopted a Supplementary Data Protection Act, while the African Union (AU) has adopted a Convention on Cyber Security and Personal Data Protection. However, while other aspects of data protection law are more or less addressed in these instruments, relatively very little focus is put on managing and safeguarding personal data security.

This paper, in an attempt to present a critique of the state of affairs as regards personal data security regulation and online trustworthiness in Africa, strives to show that the above African instruments do not provide a satisfactory response to current personal data security challenges Africa faces. Both instruments can hardly be said to ensure a trustworthy environment for data sharing, as they lack essential pre-breach and post-breach regulation mechanisms, including breach reporting, liability for mismanagement of personal data and available remedies for affected data subjects. The paper concludes by recommending that these deficiencies be addressed in additional protocols to these instruments or in relevant future texts.

Keywords: Personal data protection · Personal data security · Africa · African Union · ECOWAS

1 Introduction

Ever since the beginning of the 21st Century, Africa has had its fair share of ICT penetration, especially in terms of internet and mobile telephony usage. The continent hosted about 453 million internet users by the end of 2017 as opposed to about

R. Zitouni et al. (Eds.): AFRICOMM 2019, LNICST 311, pp. 38–58, 2020.
https://doi.org/10.1007/978-3-030-41593-8_4

4 million by 2000, and the Information Technology Union (ITU) estimates 781 million mobile phone subscriptions in the continent in 2018[1]. Africans are increasingly using the Internet for information society goods and services, ranging from online banking to social networking [1, 2]. Besides being a primary means of communication for most Africans, mobile phones have become a source of significant economic growth and a platform for innovation, especially with the rise of mobile money services: the use of mobile phones to purchase goods or services through funds connected to the user's account [3]. Mobile banking has also been on the rise in the continent for close to a decade now [4], and in 2017, mobile technologies and services generated 7.1% of GDP across Sub-Saharan Africa, a contribution that amounted to $110 billion of economic value added [5]. Mobile application usage for urban transportation is also fairly advanced in some African countries, with, for example, US-based urban transport giants Uber operating in South Africa, Kenya, Nigeria, Tanzania, Uganda, Ghana and Egypt. The so-called Internet of Things[2] is also on the rise, with an estimated 29 billion connected objects by 2022 [6]; objects being reliably connected to each other with the ability 'to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment' [7]. The emergence of 'information ambient environments', is also anticipated, characterised by invisible (i.e., embedded) computational power in everyday appliances and other common physical objects, including mobile and wearable devices where, in essence, people are surrounded with intelligent and intuitive objects capable of recognizing and responding to our presence in a seamless, unobtrusive and even invisible way [8].

As it keeps on embracing ICT usage and internet penetration, and also consequently generating huge amounts of (personal and non-personal) data, the African continent will soon get caught up in this forecasted digital hurricane. This has raised concerns at regional and sub-regional governance forums not only about the safety and security of critical ICT infrastructure and systems which are always vulnerable to cyber attacks [9, 10] but also about protecting the privacy of Africans as regards the personal information which they share over these platforms. The rapid growth of mobile telephony in Africa, for example, has barely been accompanied by appropriate consideration for privacy and security concerns, opening the door for abuse and erosion of the application's utility [11]. Just as was the case in Europe with the advent of computer processing in the 1970s culminating in the adoption of Convention 108 by the Council of Europe on 28 January 1981[3], and later the EU Directive

[1] ITU GLOBAL AND REGIONAL ICT DATA, retrieved from https://www.itu.int/en/ITUD/Statistics/Documents/statistics/2018/ITU_Key_2005-2018_ICT_data_with%20LDCs_rev27Nov2018.xls. Accessed 5/5/2019.

[2] Defined by Stuckmann, Peter, and Rainer Zimmermann in: "European research on future internet design." *IEEE Wireless Communications* 16, no. 5 (2009): 14 as a 'world-wide network of uniquely addressable and interconnected objects, based on standard communication protocols". This enables applications involving real-world objects, but also business applications based on network-assisted machine-to-machine interaction.

[3] The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28th January 1981.

95/46/EC[4] on October 24, 1995 [12, 13], African leaders, by the end of the first decade of the 21st Century, began identifying the need to protect the privacy and security of personal data of users being processed by service providers using ICTs. The first African multilateral legal framework to directly address personal data privacy protection was the ECOWAS[5] Supplementary Act A/SA./1/01/10 on Personal Data Protection within ECOWAS (hereinafter ECOWAS Data Protection Act), adopted in Abuja on February 16, 2010. This was followed by the African Union Convention on Cybersecurity and Personal Data Protection, adopted in Malabo on June 27, 2014. It should be pointed out that these instruments were being adopted at a time when some African states were also adopting or had already adopted national legislations focused on personal data protection [14] and personal data security. However, national personal data security initiatives are beyond the scope of this paper, which seeks to examine Africa's multilateral legal frameworks on personal data protection with a view of assessing whether they provide a solid basis for efficient personal data security in the face of current technological developments gradually engulfing the continent, and based on which national instruments can conceive adequate laws and policies.

The paper will point out that both the ECOWAS Data Protection Act and the AU Convention on Cyber Security and Personal Data Protection, in relation to contemporary realities of the digital environment or as compared to what obtains in Europe, do not provide a satisfactory legal springboard to guarantee an adequate level of personal information security for African citizens in the face of current data security risks posed by the continent's wide adoption of new technologies. These instruments, however, especially the AU Convention, should nevertheless be lauded for at least providing a commendable basis which could serve as a beginning for those African states which continue to embrace digital and mobile technologies without safeguarding their citizens' fundamental rights with any national framework at all bearing on personal data protection or security.

This introduction shall be followed by a first section briefly discussing the concepts of personal data, personal data protection and personal data security, and a second section briefly discussing the current dangers to personal data security in Africa. A third section shall briefly introduce the ECOWAS and AU Data Protection Conventions, and briefly discuss how they address personal data security. A fourth section identifies and discusses the aspects of personal data security absent from the Act in comparison with the European data protection model, and the fifth and final section features the author's conclusive remarks.

2 Personal Data, Data Protection and Data Security

This section briefly introduces the concepts of personal data protection and personal data security. It shall basically be a rundown of current literature on both concepts.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[5] Economic Community of West African States.

2.1 Personal Data

Personal data is the yolk of personal data protection law; the latter is triggered only if personal data is processed. It is therefore crucial for individuals, their representatives and data processing entities to understand what personal data is exactly, in order to know whether a particular operation or situation falls under the regulatory scope of data protection law.

Personal data, as it is used in Europe and (adopted in) Africa, is also known as personal information or, in the United States, personally identifiable information [15]. The first internationally-established conceptualisation of the term 'personal data' was enshrined in the OECD[6] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980. Paragraph 1(b) of the Guidelines defines personal data as 'any information relating to an identified or identifiable individual (data subject)'. The Council of Europe followed suit, adopting the very same definition in its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in Strasbourg on 28 January 1981. In the European Union, the General Data Protection Regulation adopts the very same definition, with further clarifications. It states that personal data is '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.'[7] This covers a broad range of data, from the name, date of birth, address, health records, social security numbers, driver's licence data and even the real time location of a person, and beyond. In essence, all data through which an individual is or can be identified. This definition, which also featured almost word-for-word in the repealed 1995 EU Data Protection Directive, has already been criticised for being too broad and could include virtually sort of information. The terms 'any information' and 'relating to' suggest that all sorts of information leading even slightly to a person could be 'personal', especially considering that current and anticipated computer technologies with unprecedented analytical capacities could make use of virtually any piece of information to identify a natural person, hence the risk of making every information personal data [16]. But it has also been defended on grounds that the EU legislator had as mission to provide a high standard of protection for individuals with regard to the processing of their personal information[8].

A very identical definition to the above EU definitions on personal data has been taken up by both the ECOWAS and AU data protection instruments. The ECOWAS Act defines personal data as '*any information relating to an identified individual or*

[6] The Organisation for Economic Cooperation and Development.

[7] Article 4(1), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)).

[8] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal* Data (Adopted on 20th June 2007).

who may be directly or indirectly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity (Article 1), while the AU Convention refers to it as '*any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity*.' (Article 1). From the terms 'any information' and 'relating to', it appears both instruments appear to reinforce the EU model of covering a broad range of information under the category of personal data which should be protected under the legal mechanism of personal data protection.

2.2 Personal Data Protection

Hustinx posits that personal data protection refers to that set of policies and rules which aim to protect individuals (citizens, consumers, workers, etc.) against unjustified collection, recording, use and dissemination of their personal details [17]. The concept has been particularly trendy in the US and in Europe over the last decades, following the (global) realisation that personal data plays increasingly important role in our economies and is being generated, gathered and processed at alarming rates due to wide range of analytics that can provide comprehensive insights into individuals' movements, interests, and activities[9]. Such use of personal data, if not regulated, could expose individuals to a number of risks ranging from privacy violations to serious injuries like identity theft [18]. In Europe, with the human right to private life (of the home and correspondences)[10] proving increasingly difficult to guarantee with the advent and increased use of ICTs to process personal information, there was the need for a novel regime to introduce safeguards which should be observed by organisations and institutions when processing personal information within the context of an information society [12, 19]. One of such safeguards is the requirement to ensure the security of personal data which these companies or institutions are processing.

In addition to Hustinx's definition above, it should equally be pointed out that contemporary data protection law also targets online trust i.e. making individuals feel confident and safe to share their personal data. Prior to the post-2010 data protection law reforms in the EU and US, the 'notice and consent' model was relied on to protect individuals' privacy by letting them choose, through 'informed, freely given and specific' consent whether or not to allow the processing of their personal information [20]. After 2010, following the established shortcomings of this model, especially considering, inter alia, the processing of data by third parties who were not in any direct relationship with individuals, decision or notice fatigue [21] or the unrealism to always expect data controllers to request consent to process data for purposes other than the original purpose for which it was collected, there was a shift towards equally ensuring

[9] See the OECD Privacy Framework. Retrieved from http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 2/11/2019. Page 20.

[10] Article 8 of the European Convention on Human Rights of 4 November 1950.

responsible and trustworthy use of personal data.[11] Considering that data sharing is essential for the exchange of goods and services and economic functioning of any society, data protection is therefore not just about protecting individuals but also about ensuring economic growth. The European Commission, for example, stated that contemporary EU data protection law is poised to 'help stimulate the Digital Single Market in the EU by fostering trust in online services by consumers…'[12] while Lynskey points out that EU data protection law simultaneously pursues dual objectives: economic—to facilitate the establishment of the internal market—and rights-based—to protect fundamental rights when personal data is processed [13]. In this light, and in line with the OECD Guidelines, the following principles were formulated by EU data protection law:

- Principle of lawfulness, fairness, and transparency: personal data shall be processed lawfully, fairly, and in a transparent manner.
- Principle of purpose limitation: personal data shall be collected for specified, explicit, and legitimate purposes.
- Principle of data minimization: Processing of personal data must also be adequate, relevant, and limited to what is necessary.
- Principle of accuracy: Personal data being processed must be accurate and kept up to date.
- Principle of storage limitation: Personal data is to be kept in a form that hinders identification of data subjects for no longer than is necessary for the originated purpose.
- Principle of integrity and confidentiality: Processing should appropriate security personal data.
- Principle of accountability: The data controller (person in charge of processing personal data) should always be ready to demonstrate compliance with all the above principles.[13]

2.3 Personal Data Security

Paragraph 11 of the OECD Privacy Guidelines, titled the Security Safeguards Principle, requires personal data to be '*protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data*.' Personal data security hence refers to the mechanisms undertaken to safeguard of personal information under processing by service-providing companies or institutions from unauthorised access, loss, destruction, alteration or any other circumstance which could negatively affect the processed data.

[11] See the White House, 'Executive Office of the President. Big Data: Seizing Opportunities, Preserving Values' (2014). 55–56. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. Accessed 2/11/2019.

[12] European Commission Joint Statement on the final adoption of the new EU rules for personal data protection. (Brussels, 14 April 2016). Available at https://europa.eu/rapid/press-release_STATEMENT-16-1403_de.htm. Accessed on 3/6/2019. Also see Recital 7 of the GDPR.

[13] See Article 5, GDPR.

With personal data being, *prima facie*, information in the first place, consists a subset of the broader concept of information security. The International Standardisation Organisation defines information security as the preservation of the confidentiality, integrity and availability of information, noting that information can take on many forms: it can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films, even conveyed in conversation (ISO/IEC 27002, 2005). Arguing that this definition was limited to industry standards and do not consider contemporary information security challenges, Whitman and Mattord [22] add accuracy, authenticity, utility and possession to the list of data security features.

Personal data security thus incorporates the above processed vis-à-vis information which relates to or identifies an individual. This is reflected in the European Commission's definition of personal data security breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed…"[14]. Conceptually, the term incorporates the procedural engagements taken by organisations to prevent these mishaps from befalling the personal data they process. Such engagement is crucial in any contemporary society, as compromised personal data could be used for a broad range of malpractices including impersonating the individual (identity theft) and making fraudulent transactions, or for abusive marketing, phishing or spying, which could lead to financial loss and emotional distress suffered by the concerned individual [18].

Compared to Europe and the US, personal data protection, though not really a new concept considering the existence of data protection laws in about a score of African countries today [14], is still to receive substantial media attention and legal interpretation in Africa, which is not a comfortable remark considering the continent's adoption of ICTs especially mobile telephony, and hence massive generation of personal data. The continent has generally been slow in adopting a continental privacy policy or culture, which contributes not only to the current lack of national personal data protection initiatives, but could hinder the practical enforcement of national data security legislations based on these instruments. In this light, following section discusses some inherent contextual challenges which could hinder the adequate enforcement of a personal data security framework in Africa.

3 Personal Data Security in Africa: Potential Challenges

This section briefly discusses a number of factors characterizing the African information security context, making a case for the prevalence of an informationally risky environment for African residents.

[14] Article 2(i) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

3.1 Inadequate Cybersecurity Response

The AU Convention, in its third section bearing on cybersecurity, urges Member States to, inter alia, 'elaborate and implement programmes and initiatives for sensitization on security for systems and networks users' (Article 26(1)(b)). However, many African states suffer from inadequate structures and organs to fight equipment to fight cybercrime and guarantee cybersecurity. By June 2018, though 40 out of 55 African states have adopted comprehensive cybercrime laws, only 20 States had established national cybersecurity policies, and 18 States had national CERT frameworks[15]. This inadequate cybersecurity response has eased the infection of a huge number of computers in Africa with malware: reportedly over 80% by 2010 [23]. Also, just as had been predicted almost a decade ago, a huge number of Africans now use mobile phones for mobile banking, accessing the Internet, facilitating commerce, and general communication [11].

Coupled with the inability to guarantee ICT network security, this development implies that there are huge amounts of personal data generated every day in Africa and susceptible to unauthorised access and/or misuse. Securing personal data also involves ensuring information service providers have adequate technical measures in place to safeguard the security of the network or system processing or transmitting such data. As Wayne et al. argue, key steps towards building cyber resilience in Africa should begin with implementation (of the AU Convention) and education [24], but the snail pace of ratifying the Convention so far (only five states by September 2019, since its adoption in 2014) is evidence of the apathy with which African states apparently approach cybersecurity threats and dangers.

3.2 Relatively Weak Privacy Culture in Africa

Privacy as a philosophical or even legal phenomenon has not yet received mainstream attention in Africa [25]. Some commentators even advocating that privacy is of little value in the continent, overshadowed by the togetherness community lifestyle which is dominant in local African communities [26], advocated as one of the principal features of the traditional African philosophy generally referred to as *Ubuntu* [27]. Interestingly, it is not even formally recognised by the continent's most fundamental human rights instrument: the African Charter on Human and People's Rights (ACHPR) of 1981 does not mention a right to privacy in its catalogue of basic human rights. In an effort to justify this omission of the right to privacy in the ACHPR, Olinger et al. purport that 'privacy was simply not seen as a necessary right for Africans to live freely and peaceably' [28]. On her part, Bakibinga contends that Africans generally suffer from 'privacy myopia' which means they underestimate the value of their personal data and the need for its protection [29]. It should be pointed out however that this view is not predominant among scholars: Makulilo [30] for example argues that Western influence

[15] See UNCTAD. (2018) *Cybercrime Laws.* [online] Available from: http://www.unctad.org/en/Docs/Cyberlaw/CC.xlsx [Accessed on 6 June 2018]. See ITU. (2018) *Cybersecurity Country Profiles.* [online] Available from: https://www.itu/en/ITU-D/Cybersecurity/Documents/CountryProfiles/ [Accessed 6 June 2019].

and globalization has wrought individualism in African urban areas, and privacy is becoming an evolving concept in the continent. Nevertheless, on the other hand, strong notions of privacy arose in Europe since the end of the Second World War. And while this, since the 1970s, led to advocacy for even stronger personal data protection requirements for companies processing personal data, the absence of a fundamental, continental right to privacy in Africa weakens the grounds for any such advocacy with regard to personal data [11].

This situation is not so static though: most African national constitutions do guarantee a right to privacy[16], and as discussed above, African governments have begun considering privacy protection through personal data protection laws. So far African states have been progressively adopting comprehensive data protection laws which also require security safeguards when processing personal data. These laws in question, however, are fragmented among states, portraying different standards of personal data security safeguards required of data processing organisations [31, 32]. There is also a gaping absence of public interest groups in monitor government behaviour, propose public policy, and promote privacy awareness in relation to privacy [3].

3.3 Potential for Unaccountability by African Governments

One of the core principles of data protection is accountability: personal data processing organisations or companies should always be ready to demonstrate compliance with data protection regulations.[17] Accountability towards their citizens, unfortunately, is generally not a very popular governance option among African governments [33], as many of them demonstrate a willingness to operate outside the rule of law and with little accountability [11]. The absence of a spirit of accountability provides fertile grounds for privacy violations. Contemporary literature has raised these concerns in relation to African governments. A case in point is the ongoing process of African governments in implementing comprehensive electronic ID card schemes (an example being the current 'Uduma Number' scheme by the Kenyan government). Though such initiatives may ease identification and maintain law and order, a worrying factor is that it leads to extensive databases of individuals' personal data, including sensitive and biometric data being kept by governments with virtually no national or regionally-binding personal data privacy obligations of accountability towards their citizens [34]. In the same light, Banisar for example points out that most common ICT privacy issue currently facing African nations is the development of new citizen identification systems, including identity cards and passports [35]. Even more concerning is the fact that the technical development and operation of these ID card schemes are franchised to foreign companies [34, 35] which could make claims against privacy violations difficult in terms of jurisdictional conflict.

Mass surveillance is equally another issue: African governments are extremely reticent to have any accountability or transparency of their interception and surveillance

[16] For example Article 12 of the 1996 Constitution of Cameroon, Article 28 of the revised 1992 Constitution of the Republic of Togo, Article 31 of the 2010 Constitution of the Republic of Togo.

[17] Paragraph 14 of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereinafter the OECD Data Protection Guidelines). Also Article 5(2) of the EU GDPR.

activities [36]. Some of them have even passed laws mandating telecommunication providers to integrate surveillance systems capable of interception of communications. For example, South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 requires service providers to incorporate surveillance machinery before they can offer services to the public. Section 9 of Zimbabwe's 2007 Interception of Communications Act similarly requires providers to assist with interception, while Namibia's 2009 Communications Act orders communication companies to build interceptor centres while providing little control as to who can order wiretaps [35]. A point worth noting here is that these legislations were passed to regulate traditional telecommunication systems, which are principally landline and mobile communications, and may not be compatible with the realities of the contemporary ubiquitous digital data processing. The steady advent of the IoT and even information ambient environment where all sorts of data like health, transportation or electricity consumption details can be processed by any object with censors, if not countered by strong data protection legislation, the mass surveillance capacities of African states (and their partner processor companies) on their civilians could grow to alarming levels.

This section illustrates that personal data processing in Africa presents a variety of risks to individuals ranging from unsatisfactory levels of cybersecurity, cultural privacy deficiencies or potential abuse by government or private entities. It was on this basis that African multilateral organisations (in this case ECOWAS and AU) came up with legal responses to introduce, within their respective scopes of competence, guidelines which aim to protect Africans with regard to the processing of their personal information and, in the process, ensure a trustworthy and secure online environment for the flow of personal data.

4 African Multilateral Personal Data Security Instruments

This section presents the selected multilateral instruments addressing personal data protection in Africa: the ECOWAS Data Protection Act and the African Union Convention on Cyber Security and Data Protection. It shall focus briefly on their background, scope and applicability, before discussing their provisions on personal data security.

4.1 The ECOWAS[18] Data Protection Act

ECOWAS is the main interstate organization of Western Africa with fifteen members,[19] established by the Treaty of Lagos on 28th May 1975[20]. Article 3 (2) (a) of the

[18] Established by the Treaty of Lagos on 28 May 1975, ECOWAS is the main intergovernmental organization of West Africa currently comprising of 15 sovereign West African States namely: Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, the Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mail, Niger, Nigeria, Senegal, Sierra Leone and Togo. (Www.Ecowas.Int).

[19] Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

[20] Treaty of ECOWAS (28 May 1975) 14 ILM 1200; revised 24 July 1993, 35 ILM 660, (1996).

Treaty states that Member states shall ensure the 'the harmonization and coordination of national policies and the promotion of integration programmes in areas including communications, trade, information, science, technology, services, and legal matters'. It was based on the above provision and the Supplementary Act A/SA.1/01/10 Personal Data Protection within the ECOWAS (ECOWAS Data Protection Act) was adopted during the 37th session of the Authority of ECOWAS Heads of State and Government in Abuja on 16 February 2010.

With this Supplementary Act, ECOWAS is the first and only sub-regional grouping in Africa to develop a concrete framework of personal data protection law; a framework strongly influenced by the 1995 EU Data Protection Directive. It should also be noted that Article 48 of the Act makes it an integral part of the ECOWAS Treaty, thereby making violations of the Act actionable before the ECOWAS Court of Justice. The Act has a dual objective: the protection of privacy and promotion of free movement of information[21]. It equally recognizes that technology advancements greatly ease personal data processing and hence bring about unprecedented problems of personal data protection, and seeks to address the problem through a harmonized legal framework for data protection within the ECOWAS sub-region.[22]

4.2 The African Union Convention on Cybersecurity and Personal Data Protection

Adopted by the 23rd Ordinary Session of the Assembly of Heads of State of the African Union in Malabo on 27 June 2014, the African Union Convention on Cyber Security and Personal Data Protection (the AU Data Protection Convention) provides a legal framework regulating electronic commerce, data Protection and cybersecurity. Its overall objective is to harmonise national legislation in Africa on a number of ICT-related issues; an objective which reiterates the three main AU declarations on harmonisation of ICT and related laws: the Oliver Tambo Declaration Johannesburg 2009, the Abuja Declaration 2010 and the Addis Ababa Declaration 2012 [37]. As regards personal data protection, it seeks to establish a legal framework 'aimed at strengthening fundamental rights and public freedoms, particularly the protection of [personal] data, and punish any violation of privacy without prejudice to the principle of free flow of personal data (Article 8(1) AU Convention) It is set to come into force upon ratification by 15 member states (Article 38). So far (June 2019) though, only four member states (Senegal, Namibia, Guinea and Mauritius) have ratified the Convention. After coming into force, it applies to Member states (which are mostly dualist), however, only upon the individual domestication (by Member states) into the internal law of the state.[23]

The Convention applies *rationae loci* to any automated or non-automated processing of personal data carried out in a territory of an AU Member State (Article 9(1)). However, just like Article 3(2) of the 1995 EU Directive, the Convention does not apply to data processing carried out by an individual in the exclusive framework of

[21] Paragraph 10, Preamble, ECOWAS Data Protection Act.

[22] Paragraphs 8–11, Preamble, ECOWAS Data Protection Act.

[23] See for example Section 12 of the Constitution of the Federal Republic of Nigeria.

their personal or domestic activities (Article 9(2)(a)). The Convention also covers processing of personal data for in cases of public security, defence, investigation and prosecution of criminal offences, but subject to the provisions of other existing laws (suggestively regional or national texts operating *lex specialis*) (Article 9(1)(d)).

4.3 Personal Data Security Guarantees Under Both Instruments

Both the ECOWAS Data Protection Act and AU Data Protection Convention provide for means aimed at ensuring that processed personal data is handled securely by data controllers and processors.

4.3.1 Confidentiality and Security of Processing

Firstly, both instruments contain a *Principle of confidentiality and security* when processing personal data (Article 28 ECOWAS Data Protection Act, Article 13 AU Convention), requiring data to be processed confidentially, and protected in particular when processing includes transmission of the data over a [computer] network. This principle is not very explicit under the African data protection regimes, and reference can be made to Convention 108 for a more explicit version of the principle. Article 7 of Convention 108 demands that state parties 'provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data'. Similar obligations are demanded of the data controller and processor under the GDPR.

In Africa, similar to the position of Convention 108, the onus of compliance to this principle falls generally on the data controller, whom the ECOWAS regime expressly puts in charge of ensuring the confidentiality of processing (Article 42) and obliges to "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." (Article 43). The data controller has got identical responsibilities under the AU Convention (Articles 20 and 21). Both instruments also make the data controller remains the sole responsible entity to guarantee data security, as it is up to the latter, when recruiting a processor, to ensure that the latter is equipped with sufficient guarantees for data security (Article 29 ECOWAS Data Protection Act, Article 13 (b) AU Convention). This, position, it should be noted, is slightly different from what presently obtains in Europe under the GDPR, which provides for the possibility of the processor being individually responsible for processing in the event where it acted outside the processing instructions of the controller (Article 82 GDPR).

4.3.2 The Data Protection Authority

Another data security guarantee finds expression in the wide powers granted by both instruments to the Data Protection Authority (DPA) to promote security compliance and deter non-compliance. Hustinx underlines the importance and uniqueness of the DPA by stating that data protection 'is special in the sense that it is considered to be in need of 'structural support' through the establishment of an independent authority with adequate powers and resources', while pointing out that 'no other fundamental right – except the right to a fair trial – is structurally associated with the role of an independent body to ensure its respect and further development [i.e. Courts]' [38]. In Europe, data

protection supervisory authorities have been viewed as 'an element of effective protection of individuals with regard to the processing of their personal information.[24]

Under the African data protection regimes, the DPA is entitled to receive claims and petitions relating to processing of personal data and advice petitioners on the relevant course of action to take (Article 19 (1)(f) ECOWAS Data Protection Act, Article 12(2)(e) AU Convention). He/she can hear claims of data security violations after which, in case of an emergency, he/she may suspend, block or permanently suspend proceedings (Article 19(3) ECOWAS Data Protection Act). He/she can also impose fines on a data controller who is found to be in violation of its personal data security (and, generally, data protection) responsibilities Article 20(3) ECOWAS Data Protection Act, Article 14(4)(c) AU Convention). Supervisory and enforcement institutions like the DPA will could be particularly useful in terms of creating a trustworthy online environment for data exchange in and among African countries both in terms of sanctioning defaulting data controllers who breach security principles or undermine online trust and ethics and, by virtue of their expertise in data protection law, educating data subjects on their rights towards achieving a trustworthy and secure digital environment for data sharing.

4.3.3 Right of Access and Rectification

Both instruments also provide for a right of access to data processing for individuals (Article 38 (6) and Article 39 ECOWAS Data Protection Act, Article 17 AU Convention) which is basically a right of the individual to request the data controller to present him with his data being processed by the latter as well as any information about the recipients to whom the data has been disclosed. This, at least in theory, gives individuals a chance to ensure their personal data has not been altered, providing them with some level of supervisory powers alongside the data controller. Data alteration being a data security issue in terms of data integrity[25], the right of access actually acts as a complementary security measure.

The above are the main personal data security guarantees under both the ECOWAS Data Protection Act and the AU Data Protection Convention. They admittedly cover some salient aspects in the domain, but these guarantees are quite limited in relation to the contemporary privacy demands of a data-driven society which Africa is slowly but surely becoming.

5 Some Data Security Mechanisms Missing from the Above Instruments

This section reviews the data security weaknesses of the above African multilateral data protection instruments. It shall identify and briefly discuss significant personal data security mechanisms missing from their provisions.

[24] Preamble, Additional Protocol to the Council of European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.

[25] See the EU Article 29 Working Party Opinion 03/2014 on Personal Data Breach Notification (WP213), p. 3.

5.1 Absence of a Security Breach Notification Requirement

Breach notification as a measure of personal data security management has been around for quite a while in data protection legislations, and constitutes an essential tool in ensuring responsible data processing on the part of data controllers. In essence, it requires personal data controllers or processors to inform either the competent Data Protection Authority or data subjects of a security incident which affects or is likely to have affected the personal data being processed. It was first passed into law in the US state of California in 2002 [39], and has been taken up by other states and jurisdictions, including the European Union (first by the e-Privacy Directive[26] in 2002, and later the GDPR in 2016), and is even embodied in Paragraph 15(c) of the OECD Revised Recommendation of the Council governing the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 11 July 2013.

Security breach notification rules have been established to serve three main advantages: 'they provide a systematic feedback about the actual risk and the actual weaknesses of existing security measures; they enable authorities and consumers to assess the relative capabilities of data controllers with respect to data security; they force data controllers to assess and understand their own situation regarding security measures'[27]. In other words, personal data breach reporting serves *ex ante* (shaping the future behaviour of data controllers via deterrence) and *ex post* (mitigating the harm of the breach) objectives [40]. Such mitigation could be very crucial in event of the compromise of highly sensitive data; for example, informing individuals there has been a breach so they can quickly change information like passwords or passcodes to prevent identity theft or other related criminal activity [41]. It also ensures accountability of the data controller in data processing[28] [42].

This measure feature is absent from both the ECOWAS and AU data protection instruments: they do not provide for an obligation for data controllers to inform the DPA or individual data subjects about security incidents which may have led to a loss or unauthorised access by an external body to the personal data they are processing. Though out of the scope of this paper, it should be mentioned here however that among those which have currently adopted personal data protection legislations, data security breach notification requirements currently exist some African states including Chad, Ghana, Lesotho, South Africa and Uganda. Nevertheless, its absence in the main continental instrument on personal data protection remains significant.

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[27] European Commission, Commission Staff Working Paper SEC (2012) 72 final. Impact Assessment Accompanying the General Data Protection Regulation (2012) p.100.

[28] The principle of accountability requires controllers to be able to actively demonstrate compliance to personal data protection rules without waiting on data subjects or supervisory authorities to point out shortcomings.

5.2 No 'Data Protection by Design' Requirements

Contemporary trends in data protection law, especially as regards data processing using ICT systems, and in order to ensure trustworthy processing, demand that such protection to be considered at the moment of designing the system or product [43]. In the same light, the OECD Revised Recommendations demand that personal data controllers should have in place a 'privacy management program' in charge of ensuring adherence to all the requirements of the Recommendations (Paragraph 15(b)). The EU also has similar provisions, which were in force before the adoption of the ECOWAS and AU data protection instruments.[29]

As Cunningham notes, regulations protecting privacy and personal information simultaneously encourage data security – as well as incentivize those entities that provide data security [44]. And over the years, a number of privacy enhancing technologies (PETs) have been developed in order to achieve information privacy goals especially alongside new technologies such as cloud computing and IoT, and include services like virtual private networks, transport layer security, DNS security extension, or onion routing [45]. These also include techniques like encryption, anonymisation or pseudonymisation [46]. These technologies aim at ensuring the security of communications as well as the preservation of the identity of a user in instances when such information is not required by another party, hence playing an important part in increasing the privacy and security of users and the data transmitted or processed.

Contemporary data protection law, like the EU GDPR (Article 25) for example requires processing systems which process personal information to be conceived around these PETs to guarantee 'automatic' data protection. The ECOWAS and AU data protection instruments are both silent on this aspect, apparently leaving it entirely up to data controllers to determine whether or not to employ the usage of privacy enhancing technologies when processing personal data using ICTs. Nevertheless, this mechanism is provided for by some African national legislations.[30]

5.3 Relatively Vague General Security Standard of Data Processing

Similar to the above point on PETs, the wordings of the ECOWAS and AU data protection instruments set relatively weak data security standards in safeguarding personal data processing, compared to what obtains in Europe, for example. Vaguely requiring that personal data be "processed confidentially and protected", (Article 28 ECOWAS Data Protection Act, Article 13 AU Convention) they appear to leave the methods and level of protection to be determined entirely by the data controllers, giving no guidance as to what technical or administrative measures to take to guarantee security. It could be argued though that, by interpretation, determining whether or not personal data is adequately protected depends on the type of data and the threats such data is likely to be exposed to, hence there could be no further need to stress on the

[29] Recital 46 of EU Directive 95/46/EC adopted in 24th October 1995 requires data security measures be taken at the time of designing the processing system as well as during processing itself.

[30] See for example Article 25 of the Ghanaian Data Protection Act 2012 and Article 41 of the Kenyan Data Protection Bill 2019.

measures to take, as the data controller is expected to know the kind of protection appropriate for protecting the data being collected and processed. In other words, how 'secure' a particular processing activity is shall depend on the type of data and risks involved with such processing, data protection having been portrayed by some commentators as a risk-management kind of legal regime [47].

However, this appears to put too much trust in the data controllers, which is risky business because most data processing bodies are privately-owned businesses, and hence are inherently inclined on maximizing profit which could be at the expense of implementing state of the art privacy protection mechanisms. The EU, for example, adopts the same risk-management standard to securing personal data, but goes ahead to lay further guidance as to how a data controller or processor determines if it has put in place adequate security measures. Article 17 of the 1995 Data Protection Directive states that data controllers must "ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected…taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected."[31] Similar to the principle of confidentiality and security of processing discussed in Sect. 3 above, the European approach is much more explicit and lays down guidelines to prove secure processing: state of the art of the security component available on the market, and the cost of its implementation (consideration whether the cost of implementing the security measure is not too superfluous). This provides more explicit guidance to data controllers in knowing what types of security measures to adopt to show compliance.

5.4 No Reference to Certification Schemes

Both African international instruments do not provide for certification schemes through privacy seals. In brief, a privacy seal is a certification mark or a guarantee issued by a certifying entity verifying an organisation's adherence to certain specified privacy standards that aim to promote consumer trust and confidence [48]. Already functional in Europe, privacy certification seals are issued by organisations (known as certification bodies) accredited for such purposes by the competent privacy or data protection authorities. Personal data processing companies wishing to demonstrate compliance to data protection rules can apply to these organisations to be certified under such seals, which could be granted following due review and relevant inspections of their privacy policies in place. Privacy seals permit individuals to quickly assess the privacy or data security levels of the goods and services they subscribe to, as they cannot independently determine the data protection or privacy behaviour of the data controller.

Voluntary privacy certification schemes are encouraged in contemporary privacy legislations[32] as they rapidly demonstrate that certified entity's data protection (and, in parallel, data security) practices meet certain standards to the satisfaction of the certification body. Benefits of privacy seals may also include: generation of privacy and data protection accountability and oversight; enhancement of trust and confidence,

[31] Also see Article 32 GDPR.

[32] See Recital 100 GDPR.

reputational, competitive and market advantages to entities using them; generation of privacy awareness; assistance in proving fulfilment of privacy and data protection obligations [49].

5.5 No Direct Data Controller-Data Subject Liability

Another significant setback of the African multilateral response to data security problems is the absence of an established, direct liability relationship between the data controller and the data subject. The provisions of the ECOWAS and AU instruments position the data controller to be answerable solely to the DPA with respect to its data processing obligations; only the DPA can impose sanctions in event of a breach of security obligations. It appears both instruments create a direct liability relationship only between the data controller and DPA, leaving out the individuals whose data is processed and who risk direct harm in event of the compromise of his personal data. Under both instruments, the DPA is charged with receiving data protection violation claims (from individuals) and advising them on the course of action to follow (Article 19 ECOWAS Data Protection Act, Article 12 AU Convention). He appears therefore as an unwavering intermediary who decides a victim's course of action on his behalf. Considering that the very essence of data protection law is the protection of individuals regarding the misuse of their personal information, it appears only rational that data controllers be made directly liable towards them as regards protecting their personal data, so they feel protected during the processing. Leaving individuals out of a liability relationship with the data controller therefore appears a data security omission on the part of the African legislator.

5.6 Lack of a Compensation Scheme for Data Breach Victims

The above-mentioned absence of a direct liability relationship between the data controller and data subject leads to another grey area under African multilateral data protection law: compensation for victims of data security violations. Both the ECOWAS and AU data protection legislations fail to set a legal basis for Member states to enact laws which guarantee compensation for data subjects who are victims of personal data breaches. In the same light as data breach notification, such provisions would serve as an incentive for data controllers and processors to comply with standard security measures of data processing in order to at least ensure compliance. As discussed above, and unlike what obtains in other jurisdictions[33], victims are not provided with a right of direct claim against the data controller.

Also, the only monetary sanction available against the data controller under both data protection instruments is a fine, imposed by the DPA. By nature, fines are generally paid into the state treasury, or could be paid to the office of the DPA, but not to individuals. However, both instruments are silent as to any compensation mechanisms available for victims directly harmed by these security violations, which puts victims in a precarious situation: they cannot bring an action in data protection against the data

[33] See for example Recital 55 of the 1995 European Data Protection Directive.

controller, and they cannot lay a claim on a fine paid for a violation in which they suffered injury. It should be pointed out though that nothing appears to prevent victims directly claiming against the data controller on the basis of tort law.

6 Conclusive Remarks

This paper set out to provide an assessment of Africa's multilateral response, as contained in the ECOWAS Data Protection Act and African Union Data Protection Convention, to personal data security threats to which are (or would be) exposed African data subjects as Africa embraces ICTs and other tech-related innovations, occasionally comparing their provisions to European data protection frameworks in the process. Discussions centred in the first place on the notions of personal data, personal data protection and personal data security. Then an overview of the current fertility of African grounds for the adoption and implementation of standard personal data security norms was discussed, illustrating concerns revolving around the continent's weak cybersecurity institutions and fragile privacy culture and unaccountability of its governments in terms of enforcing human rights norms. This was followed by an appraisal of the current AU and ECOWAS data protection instruments, which led to the discovery that though these instruments do feature some provisions which contribute towards ensuring a secure and trustworthy digital African environment like the embodiment of a Security of Processing Principle, existence of a right of access and provision of Data Protection Authorities, they however lack other crucial safeguards to guarantee, at their respective continental and regional levels, an adequately secure and trustworthy environment which seriously limits data processing abuses from public or private entities. The safeguards identified as lacking, which include rules relating to data breach notification or data protection by design, are well guaranteed in European data protection law, and some are embodied as data processing principles in the OECD Privacy Protection Guidelines.

It can therefore be concluded that the adoption of both ECOWAS and AU instruments is an unequivocal indication of the continent's willingness and progress in protecting the personal information of its citizens from security risks related to data processing by public or private entities, and implement online trust. Both instruments do contain a principle of confidentiality and security of data processing, requiring Member States to ensure data controllers implement appropriate security safeguards when processing personal data. However, some significant security mechanisms are missing from both instruments, mechanisms which could be addressed in an additional protocol to these instruments or in future multilateral texts in view of ensuring relatively strong data security standards for African citizens, to promote a trustworthy and safer digital environment.

Acknowledgments. This research is funded by the Erasmus Mundus program LAST-JD (Joint International Ph.D. in Law, Science and Technology) coordinated by the University of Bologna.

References

1. Adesoji, A.: Mobile technology, social media and 180 million people. J. Bus. Adm. Manag. Sci. **6**, 82–85 (2017)
2. Kayisire, D., Wei, J.: ICT adoption and usage in Africa: towards an efficiency assessment. Inf. Technol. Dev. **22**(4), 630–653, 641 (2016)
3. Harris, A., Goodman, S., Traynor, P.: Privacy and security concerns associated with mobile money applications in Africa. Wash. J. Law Technol. Arts **8**, 245–246 (2012)
4. Tchouassi, G.: Can mobile phones really work to extend banking services to the unbanked? Empirical lessons from selected Sub-Saharan Africa Countries. Int. J. Dev. Soc. **1**(2), 70–81 (2012)
5. GSMA: The Mobile Economy Report 2013, p. 3. A.T. Kearney, London, United Kingdom (2013)
6. Ericson Mobility Report, June 2017. https://www.ericsson.com/en/mobility-report/internet-of-things-outlook. Accessed 26 June 2019
7. Madakam, S., Ramaswamy, R., Tripathi, S.: Internet of Things (IoT): a literature review. J. Comput. Commun. **3**(05), 164 (2015)
8. Emiliani, P.L., Stephanidis, C.: Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities. IBM Syst. J. **44**(3), 605–619 (2005)
9. Orji, U.J.: The African union convention on cybersecurity: a regional response towards cyber stability. Masaryk UJL Technol. **12**, 91 (2018)
10. Orji, U.J.: Multilateral legal responses to cyber security in Africa: any hope for effective international cooperation? In: 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon), pp. 105–118. IEEE (2015)
11. Goodman, S., Harris, A.: The coming African tsunami of information insecurity. Commun. ACM **53**(12), 24–27 (2010)
12. Fuster, G.: The Emergence of Personal Data Protection as a Fundamental Right of the EU, vol. 16. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05023-2
13. Lynskey, O.: The Foundations of EU Data Protection Law. Oxford University Press, Oxford (2015)
14. Rich, C.: Privacy laws in Africa and the Middle East. The Bureau of National Affairs, editor. Privacy and security law report. BNA, Bloomberg (2015)
15. Schwartz, P.M., Solove, D.J.: The PII problem: privacy and a new concept of personally identifiable information. NYUL Rev. **86**, 1814 (2011)
16. Purtova, N.: The law of everything. Broad concept of personal data and future of EU data protection law. Law Innov. Technol. **10**(1), 40–81 (2018)
17. Hustinx, P.: EU data protection law: the review of directive 95/46/EC and the proposed general data protection regulation. Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, pp. 1–12 (2013)
18. Solove, D.J.: The new vulnerability: data security and personal information. In: Chander, A., Gelman, L., Radin, M.J. (eds.) Securing Privacy in the Internet Age. Stanford University Press, Palo Alto (2008)
19. De Hert, P., Gutwirth, S.: Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) Reinventing Data Protection?, pp. 3–44. Springer, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_1
20. Mantelero, A.: The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Comput. Law Secur. Rev. **30**(6), 643–660 (2014)

21. Soeder, M.O.: Privacy challenges and approaches to the consent dilemma. Masters thesis. SSRN 3442612 (2019)
22. Whitman, M., Mattord, H.: Principles of Information Security. Thompson Course Technology, Boston (2009)
23. Gady, F.: Africa's cyber WMD. Foreign Policy, 24 March 2010
24. Dalton, W., van Vuuren, J.J., Westcott, J.: Building cybersecurity resilience in Africa. In: 12th International Conference on Cyber Warfare and Security 2017 Proceedings, pp. 112–120. Academic Conferences and Publishing International Limited, Reading (2017)
25. Makulilo, A.B.: The Context of Data Privacy in Africa. In: Makulilo, A.B. (ed.) African Data Privacy Laws. LGTS, vol. 33, pp. 3–23. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47317-8_1. (citing Westin's Privacy and Freedom (1967)
26. Makulilo, A.: Privacy and data protection in Africa: a state of the art. Int. Data Priv. Law **2**(3), 163–178 (2012)
27. Kamwangamalu, N.M.: Ubuntu in South Africa: a sociolinguistic perspective to a pan-African concept. Crit. Arts **13**(2), 24–41 (1999)
28. Olinger, H.N., Britz, J.J., Olivier, M.S.: Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa. Int. Inf. Libr. Rev. **39**(1), 31–43 (2007)
29. Bakibinga, E.M.: Managing electronic privacy in the telecommunications sub-sector: the Ugandan perspective. In: Africa Electronic Privacy and Public Voice Symposium (2004)
30. Makulilo, A.B.: A person is a person through other persons-a critical analysis of privacy and culture in Africa. Beijing L. Rev. **7**, 192 (2016)
31. Rich, C.: Privacy laws in Africa and the Near East. The Bureau of National Affairs, editor. Privacy and security law report. BNA, Bloomberg, September 2017
32. Rich, C.: Privacy laws in Africa and the Middle East. The Bureau of National Affairs, editor. Privacy and security law report. BNA, Bloomberg, June 2015
33. Adejumobi, S.: Engendering accountable governance in Africa. In: International Institute for Democracy and Electoral Assistance (IDEA) and Development Policy Management Forum (DPMF) Regional Conference on "Democracy, Poverty and Social Exclusion": Is Democracy the Missing Link (2000)
34. Abdulrauf, L.A., Fombad, C.M.: The African Union's data protection convention 2014: a possible cause for celebration of human rights in Africa? J. Media Law **8**(1), 67–97 (2016)
35. Banisar, D.: Linking ICTs, the right to privacy, freedom of expression and access to information. East Afr. J. Peace Hum. Rights **16**(1) (2010)
36. Sutherland, E.: Digital privacy in Africa: cybersecurity, data protection & surveillance. LINK Centre (2018)
37. Makulilo, A.B.: Myth and reality of harmonisation of data privacy policies in Africa. Comput. Law Secur. Rev. **31**(1), 78–89 (2015)
38. Hustinx, P.: The role of data protection authorities. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) Reinventing Data Protection?, pp. 131–137. Springer, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_7
39. Stevens, G.M.: Data security breach notification laws. Congressional Research Service (2012)
40. Esayas, S.: Breach notification requirements under the European Union legal framework: convergence, conflicts, and complexity in compliance. John Marshall J. Inf. Technol. Priv. Law **31**, 317–368 (2014)
41. Schwartz, P., Janger, E.: Notification of data security breaches. Mich. Law Rev. **105**, 913 (2006)
42. Boillat, P., Kjaerum, M.: Handbook on European Data Protection Law, p. 77. Publications Office of the European Union, Luxembourg (2014)

43. See for example Paragraph 44, EU Article 29 Working Party. The future of privacy, WP 168. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf. Accessed 1 December 2009
44. Cunningham, M.: Privacy in the age of the hacker: balancing global privacy and data security Law. George Wash. Int. Law Rev. **44**, 643 (2012)
45. Weber, R.H.: Internet of things: privacy issues revisited. Comput. Law Secur. Rev. **31**(5), 618–627 (2015)
46. Europa, Privacy Enhancing Technologies (PETs), 2 May 2007. http://europa.eu/rapid/pressrelease_MEMO-07-159_en.htm. Accessed 24 Feb 2019
47. Gellert, R.: We have always managed risks in data protection law: understanding the similarities and differences between the rights-based and the risk-based approaches to data protection. Eur. Data Prot. L. Rev. **2**, 481 (2016)
48. Rodrigues, R., Wright, D., Wadhwa, K.: Developing a privacy seal scheme (that works). Int. Data Priv. Law **3**(2), 100–116 (2013)
49. Rodrigues, R., Barnard-Wills, D., De Hert, P., Papakonstantinou, V.: The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. Int. Rev. Law Comput. Technol. **30**(3), 248–270 (2016)