Consolidating the Right to Data Protection in the Information Age: A Comparative Appraisal of the Adoption of the OECD (Revised) Guidelines into the EU GDPR, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019

Rogers Alunge(✉)

Joint International PhD in Law, Science and Technology (LAST-JD) CIRSFID, University of Bologna, Bologna, Italy
alungerogers@yahoo.com

Abstract. The proliferation of ICTs and computational power in processing personal information has long been documented to expose individuals to risks of privacy violations and other fundamental rights abuses. This prompted calls, about five decades ago, for the development of legal regimes laying specific rules to follow when processing personal information, especially with the use of ICTs, in order to protect fundamental individual rights. Deliberations in this direction were undertaken at the OECD, and led to the adoption of the OECD Guidelines of Privacy Protection in September 1980 (revised in July 2013), which listed eight principles of data processing on which national and supranational regimes were expected to build personal data processing laws.

This paper attempts a comparative review on how these principles are consolidated in relevant European and African legislation: that is, between the EU's GDPR on the one hand and the Ghana and Kenyan data protection instruments on the other. Being a more advanced legal regime in terms of data protection, the GDPR serves here as a measuring rod to examine how the basic OECD Principles are reflected in the personal data processing rights and obligations provided in the Ghana Data Protection Act of 2012 and the Kenyan Data Protection Act of 2019. The paper concludes with a general note that while the Kenyan legislation appears mostly copied from and consolidates OECD data protection principles more or less exactly like the GDPR, the Ghanaian Act offers comparatively less rigorous protection in some areas.

Keywords: Data protection · GDPR · Ghana Data Protection Act · Kenya Data Protection Act · OECD

1 Introduction

As the world keeps adopting innovations in Information and Communication Technology (ICT) and other forms of computational machinery to facilitate human interactions, the

J. P. R. Thorn et al. (Eds.): InterSol 2020, LNICST 321, pp. 192–207, 2020.
https://doi.org/10.1007/978-3-030-51051-0_14

last few decades are equally witnessing a global shift by national, international and supranational legal regimes increasingly giving individuals some level of control over information about themselves processed by means of ICTs. Following the documentation of the ever growing risks people expose themselves to as they increasingly rely on ICTs and other technologies [1, 2, 3], the reaction by main legal frameworks has been to impose some rules to be observed and rights to be considered when processing information about individuals. We are in a time when governments and private bodies are enthusiastically investing in the use of 'Big Data' analytics to solve governance problems or study consumer behaviour respectively, and there is a high demand for 'smart' technologies as well as the unprecedented generation of personal information by every web click or online activity. In the midst of all the hype about the praiseworthiness and added value which technology and personal information processing has added to humanity, there have also been concerns about the implications of the extensive monitoring and/or surveillance of our online activities by multilateral institutions and governments [4].

These concerns began mainly following the increasing use of computational power to process information in the 1960s and 1970s, and were mainly privacy concerns [4], but soon it became apparent that the traditional right to privacy may not be adequate to guarantee the necessary safeguards for other fundamental rights of individuals in a context of easy data generation, processing and recycling with the aid of sophisticated ICTs. This led to calls for enhanced protection over personal information [5], to be implemented through imposing certain restrictive or security obligations on public or private institutions processing personal data, while simultaneously granting individuals some rights geared towards exercising some level of control over the information about them being processed by these institutions.

In light of these developments, the 1970s witnessed the emergence of a novel set of principles aimed at protecting the fundamental rights and freedoms of individuals in a context of ubiquitous ICT proliferation. These principles were first embedded in the OECD[1] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23rd September 1980, and are generally referred to as principles of 'personal data protection' (in Europe and later Africa) or 'information privacy' (USA) [6]. This relatively novel legal regime sought to provide safeguards whenever information about individuals is being processed, and especially where such processing is done using ICTs — based on the conviction that the extensive use of ICTs for this processing data could have far reaching effects for the rights and interests of individuals. [7]. In terms of scope, the Guidelines apply to any personal data whose processing, whether by a public or private body or through automation or manually, poses a danger to privacy and individual liberties (Article 2, OECD Guidelines). It defines personal data 'any information relating to an identified or identifiable individual (data subject)'[2], subjecting its processing to eight 'principles': the collection limitation principle, the data quality principle, the purpose specification principle, the use limitation principle, the security safeguards principle, the

[1] The Organisation for Economic Co-operation and Development is an intergovernmental economic organisation with 36 member countries, founded in 1961 to stimulate economic progress and world trade. See www.oecd.org. Accessed 14/9/2019.

[2] Article 1(b), OECD Revised Guidelines 2013.

openness principle, the individual participation principle, and the accountability principle. On 11 July 2013, the OECD Council adopted a revised edition of the Guidelines. The eight Principles of the original version remained unchanged, but some new principles were added, including: National Privacy strategies, Privacy management programmes, and Data security breach notification.

National and supranational legal responses to privacy and data protection risks have been developed around these Guidelines. Reason why data protection laws exist in over 120 countries worldwide including 25 African countries [8], and instruments have been introduced by international and regional institutions such as the European Union, ECOWAS[3] and the African Union[4]. It should be pointed out that legal literature has constantly discussed the relationship between the concepts of privacy and data protection in the information age, with scholars still debating as to whether they are two dimensions to the same right or two distinct rights founded on different principles. While Bignami [9] considers data protection generally as a means to guarantee the right to privacy in the information age, Lynskey [5] appears in favour of their interpretation as two separate though heavily interlinked concepts and rights, while de Hert and Gutwirth [10] acknowledge that the former was conceived to address the shortcomings of the law to guarantee the right to privacy in an increasingly digitised era, a view Solove [11] equally shares. Without dwelling much on this debate, this paper adopts, for a definition of data protection, the position of the Council of Europe's convention 108 as interpreted by Hustinx [7], as those set of rules observed when processing personal data in order to protect the fundamental rights and freedoms of persons (including privacy) from any eventual violation.

In light of the above, this paper intends to review, at a higher level of abstraction, how the data protection principles embedded in the OECD Guidelines are incorporated within the European legal framework as opposed to African national responses. In particular, it comparatively examines the consolidation of these principles in Europe's General Data Protection Regulation (GDPR) on the one hand, and their materialisation in the Ghana Data Protection Act 2012 and Kenyan Data Protection Act 2019 on the other hand. The intention is, in the end, to formulate an appraisal of the level of personal data protection available to Ghanaian and Kenyan residents as opposed to their European counterparts.

This introduction shall therefore be followed by a second section briefly reviewing the events leading to the conception, adoption and subsequent revision of the OECD Privacy Guidelines. A third section shall briefly present the GDPR, the Ghanaian and Kenyan data protection instruments. The fourth section, the main part of the paper, shall examine the consolidation of the OECD Principles of data processing under all three instruments with the aim of identifying the similarities and differences between the European and African instruments, followed by a fifth and final section dedicated to conclusive remarks.

[3] Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS.

[4] African Union Convention on Cyber security and Data Protection, 2014.

2 The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The OECD Guidelines was the first international embodiment of international principles regulating the processing of data—a text agreed upon both by the US and European countries[5]. The build-up towards its adoption can be said to have concretely began in 1972 with the creation of a Data Bank Panel within the OECD charged with 'reflecting on the regulation of the processing of information about individuals in automated databases' [3], which organised, in 1974, an *OECD Seminar on Policy Issues in data protection and privacy*, which had on the agenda discussions on privacy as well as harmonizing the already disparate rules relating to transborder data flows among member states. Three years later, in 1977, the Data Bank Panel organised a *Symposium on Transborder Data Flows and the Protection of Privacy*, which led to the dismantlement of the Data Bank Panel, and the creation of an Expert Group in 1978, immediately charged with the task of drafting Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data for the OECD [3]. After two years of negotiation, the Guidelines were finally adopted on 23rd September 1980.

The Recommendations of the Council on the Guidelines (to which the Guidelines were attached as annex) affirms the dual intention of the OECD member states to, through the Guidelines, protect 'privacy and individual liberties' while 'advancing the free flow' of information between member states[6]. It is worth mentioning that the Guidelines repeatedly use the term 'privacy protection' rather than 'data protection', a choice of words largely in favour of the US approach which has always formally employed the term 'informational privacy' in both US law and doctrine to refer to the legal regime established under the Principles in the Guidelines, instead of 'data protection' as it is referred to in Europe [12]. A revised version was adopted on 11th July 2013.

3 The European GDPR[7], the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019

The following subsections briefly present the European GDPR and the current Ghanaian and Kenyan data protection instruments, as well as their objectives and subject matter.

[5] See the Working Party for Information Security and Privacy (WPISP). 2011. The evolving privacy landscape: 30 years after the OECD Privacy Guidelines. Directorate for Science, Technology and Industry—Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG(2010)6/FINAL,6.4.2011. DSTI/ICCP/REG(2010)6/FINAL. P.12.

[6] Recommendations of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).

[7] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), published in Official Journal of the European Union, L 119, 4 May 2016. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 25th February 2020.

3.1 The European General Data Protection Regulation (GDPR)

Coming into force on 25th May 2018 and repealing the 1995 European Data Protection Directive[8], the GDPR is Europe's main instrument regulating the processing of personal information. It was conceived to 'ensure a robust protection of the fundamental right to data protection throughout the European Union and strengthen the functioning of the [European] Single Market'[9]. It establishes rights to guarantee and obligations to comply with when processing information about or relating to individuals located within the European Economic Area, or where such processing is done by an entity located within the latter. Being a Regulation, it is directly applicable and enforceable in EU Member States according to Article 288 of the Treaty on the Functioning of the European Union (TFEU). It is widely considered the standard to follow in terms of data protection/digital privacy, lauded as the 'most profound privacy law of our generation' for being 'majestic in its scope and ambition' due to its broad definition of personal data and its attention-grabbing penalties, among other things [13]. It however runs concurrently with the e-Privacy Directive[10] and Police Directive[11] which apply lex specialis where the processing takes place respectively over a publicly accessible telecommunication network or within the context of a criminal investigation.

3.2 The Ghana Data Protection Act 2012

The Ghana Data Protection Act entered into force on 16th October 2012, with the objective to protect the privacy of individuals with regard to the processing of (their) personal information[12]. It came up as a fortification of the right to privacy provided for by Article 18 of the 1992 Constitution, following concerns expressed by the Ghanaian Government of the risks of harm likely to befall Ghanaian citizens through the misuse of their personal information [14], especially when processed by means of ICTs [15]. It has

[8] 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, Official Journal L281, 23/11/1995, 0031–0050. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046. Accessed 25th February 2020.

[9] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for The 21st Century COM/2012/09 Final (2012). Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012DC0009. Accessed 25th February 2020.

[10] 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). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058. Accessed 25th February 2020.

[11] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680. Accessed 25th February 2020.

[12] Ghana Data Protection Act 2012.

also been commented that the Act was a manifestation of the Ghanaian government's desire to give the state a positive remark in the eyes of the EU in terms of the third country adequacy requirement of the then trendy 1995 EU Data Protection Directive (Article 25), which demanded that EU countries ensure that a third country provides an adequate level of (data) protection before transferring the data of EU citizens to that state [16]. In any case, it remains one of the first national responses by an African state to digital privacy concerns.

3.3 The Kenyan Data Protection Act 2019

The Kenyan Data Protection Act of 2019 represents Kenya's most recent and main instrument regulating the processing of personal information of Kenyan residents. The Act's historical background can be traced back to the cyber law reform process in the East African Community (EAC) of which Kenya is a member state, which began on 28 November 2006 leading to the adoption of the EAC Framework for Cyberlaws Phase I recommending EAC member states to adopt data protection legislation based upon international best practices [17]. The country later adopted a new constitution on 27th August 2010 explicitly providing for a right to privacy to include a right not to have 'information relating to their family or private affairs unnecessarily required or revealed' or 'the privacy of their communications infringed.'(Article 31). To further consolidate this right, significant attempts were made to produce a draft bill in 2012, and 2013, with the Ministry of Information and Communication Technology finally releasing, in August 2018, the Privacy and Data Protection Policy 2018 and draft Data Protection Bill, 2018. The latter was then subject to further deliberation in Parliament and later released by the Directorate of Legal Services in July 2019 as the Data Protection Bill 2019. It was signed into law by the President of the Republic on 8th November 2019, and entered into force on 25th November 2019. It consists of 75 Articles arranged into 11 parts, offering a broad range of protection to Kenyan citizens with regard to personal data processing.

4 Consolidating the OECD (Revised) Principles (and Corresponding Rights and Obligations) of Data Processing in Europe, Ghana and Kenya

This section, the main focus of this paper, reviews the incorporation of the above-mentioned OECD Principles of data processing listed in the Guidelines into the GDPR, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019.

4.1 Collection Limitation Principle (Paragraph 7 OECD Revised Guidelines)

Paragraph 7, laying down the first Principle of the OECD Revised Guidelines, states that 'there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.' Information individuals share about themselves determines the inferences society makes about their lives. This Principle hence acts like the first line of defence of individuals against inferences from data about them. With the proliferation

of ICTs and social media platforms, rise of Big Data and IoT, and companies investing hugely in data analytics, all kinds of data are used to study consumer behaviour; even data which, most at times, we do not even know exist or which we generate unconsciously [18] but could nevertheless be used to make inferences and decisions about us. Under this Principle, data controllers should have a valid, proportionately reasonable and legitimate reason for collecting personal data. Also, such data should be lawfully obtained i.e. not through fraudulent means or by harassing the individual.

In Europe, the GDPR embeds this Principle in its Article 5(1)(a), requiring personal data to be processed 'lawfully' and 'fairly', while Article 5(1)(c) demands that the data collected should be relevant and limited to the exact needs for the specific processing activity. Article 6 lays down the confines within which data can be collected for processing (consent, performance of a contract, compliance with an enforceable legislation, protecting the vital interests of an individual; public interest, or on grounds of valid legitimate interest[13] of the data controller).

In Ghana, Article 19 of the Data Protection Act, titled 'Minimality' provides that personal data 'may only be processed if the purpose for which it is to be processed, is necessary, relevant and not excessive.' Article 20(1) then lists the legal grounds for processing, which are the same as in the GDPR, listed in the same order. In Kenya, Articles 25(b) to (d) of the Data Protection Act require processing to be 'fair' and 'lawful', and personal data collection should be specific, relevant and limited to the object of processing. Article 30(1) also lists the same legal basis for data processing as in the GDPR, adding processing for historical, statistical, journalistic, literature, art of scientific research (Article 30(1)(b)(viii)).

4.2 Data Quality Principle (Paragraph 8, OECD Guidelines)

Article 8 of the OECD Guidelines requires that personal data 'be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.' It aims to prevent inaccurate and unfair decisions being taken from processing individuals' personal information [19]. For example, an individual seeking a loan could find it denied if the database consulted by the bank to check his/her creditworthiness contains inaccurate or outdated details about his/her financial situation, history or behaviour. It is up to the data controller to ensure that the information based on which decisions are taken about individuals are relevant and accurate[14].

The GDPR's Recital 39 and Article 5(d) require reasonable steps to be taken to ensure that inaccurate personal data upon which decisions are or are to be taken with

[13] 'Legitimate interest' could exist when there is a relevant relationship between the data controller and data subject, like where the data subject is a client or is at the service of the data controller (Recital 47 GDPR).

[14] This principle founded the decision of the Ninth Circuit Court of Appeal in the famous US case of *Spokeo v. Robbins*, 867 F. 3d 1108 - Court of Appeals, 9th Circuit 2017. The Court found that Mr Robbins had grounds to sue an employment placement company for having, on his profile, and for not taking the necessary steps to update inaccurate information about his marital and employment status, age and educational background, which could have been the reason why he could not find a job through that company.

regard to individuals are rectified or deleted. It also provides individuals with a right to have rectified inaccurate or incomplete data concerning them with regard to the purpose for which the data is processed (Article 16).

In Ghana, the Data Protection Act mentions 'quality of information' as a principle in its Article 17(e), and Article 26 imposes a duty on the data controller to ensure that processed data 'is complete, accurate, up to date and not misleading having regard to the purpose for the collection or processing.' In terms of related individual rights, Article 33(1) permits an individual to request the correction or deletion of 'personal data that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully…' It is interesting to note the applicability of this right in the Act vis-à-vis unlawfully obtained data: even if such data may apparently be accurate, the individual can still request its deletion if they can show it was unlawfully collected.

In Kenya, Article 25(e) of the Data Protection Act requires personal data to be 'accurate and, where necessary, kept up to date' with reasonable steps taken to ensure 'inaccurate personal data is erased or rectified without delay.' While Article 26 (d) and (e) and Article 40(1) grant individuals a right to request the correction and deletion of false or misleading data about them.

4.3 Purpose Specification and Use Limitation Principles (Paragraphs 9 and 10, OECD Revised Guidelines)

Both Paragraphs 9 and 10 of the OECD Revised Guidelines place material and time-based limits on the usage of personal data by data controllers. In essence, Paragraph 9 requires that personal data collected from an individual should be processed strictly within the confines of the purpose for which it was originally collected with no further processing, unless the individual consented to it or such further processing is clearly compatible with the original purpose or is necessary for other purposes permitted by law. For example, if an individual submits their home address to a company in order to have a service delivered to them, that company should not further use that home address for another purpose e.g. to advertise other products to the individual, unless the individual expressly consents to such further use. This principle targets the limitation of non-intuitive inferences which could be generated from further processing of personal data, which currently are not uncommon occurrences [20]. Paragraph 10 on its part limits the timeframe within which personal data can be stored by the data controller i.e. personal data should not still be kept after the specified purpose for which it was processed has been completed. This reduces the risk of processed data becoming excessive, irrelevant, inaccurate or outdated, or that the data is erroneously reused to the detriment of the individual. Practically, it helps complement the accuracy principle, which is discussed later.

This Principle is manifested in Article 5(b) of the GDPR, obliging data controllers to remain within the confines of the original purpose of processing, and can only subject the data to further processing if such secondary processing is reasonably compatible with original purpose for which the data was collected. Article 5(e) GDPR on its part brings to life Paragraph 10 of the Guidelines, with what is known as a 'storage limitation' requirement: which requires personal data, as long as it can enable the identification of an individual, should not be kept for longer than necessary (i.e. it should be kept just

for the time needed for the original processing purpose for which it was collected). It should be noted however that this is subject to exceptions of the data being processed for scientific research or statistical purposes. Nevertheless, there should always be appropriate safeguards in place to protect the rights of the data subject.' Also relevant in this respect is the right available to data subjects not to be subject to decisions based solely on automated processing of their data i.e. without any human intervention in the processing (Article 22). This prevents the data controller from using other data they may have previously (and lawfully) obtained from the data subjects to infer behavioural traits or generate digital profiles for other purposes. It should be noted though that such automatic processing is allowed provided the data subject consented to it, or if it is for the performance of a contract to which the data subject is a party.

In Ghana, Article 17(c) of the Ghana Data Protection Act demands 'specification of purpose' when processing personal data, while Article 25 requires the data controller to process data solely for the purpose for which it was collected, and any further processing must be in compatibility with the original purpose, or unless consented to or if required by law). As regards storage limitation, Article 24(1) states that data controllers, subject to exceptions inter alia like research or statistical purposes, 'shall not retain…personal data for a period longer than is necessary to achieve the purpose for which the data was collected and processed'. In terms of corresponding data subject rights, Article 41(1), however, grants a right against automated decision-making using personal data only upon a written request by or on behalf of the data subject asking the controller to refrain from using their data for such processing. And this, apparently, only if the decision 'significantly' affects the data subject. This conveys an interpretation that organisations could generate pure automated-decisions from individuals' data if the latter do not expressly and unilaterally request the contrary, or if the decision does not 'significantly' affect them. In any case, if the decision significantly affects the individual, they are entitled to a written notice by the controller, and a chance to challenge the decision (Article 41 (2)). But then, the Act establishes no test to determine when a result can be said to 'significantly' affect an individual.

Article 25(c) of the Kenyan Data Protection Act specifies that data be collected for 'explicit, specified and legitimate purpose and not further processed in a manner incompatible with those purposes' and Article 30(2) expressly obliges controllers to process personal data in accordance with the (original) purpose for processing. As regards storage time limits, the Act requires controllers and processors not to keep personal data 'for longer than is reasonably necessary to satisfy the purpose for which it processed unless authorised or required by law, is consented to by the individual or is processed for historical, statistical, artistic, journalistic or related research purposes (Article 39(1)). The Act also replicates the GDPR by granting to individuals a general right not to be subject to decisions arrived solely by automated decision-making systems (Article 35(1)).

4.4 Security Safeguards Principle (Paragraph 11 OECD Revised Guidelines)

Paragraph 11 OECD Guidelines lays down the security requirement of the personal data processing, requiring data controllers to ensure that personal data is processed securely without undesirable disclosure or compromise i.e. it should be protected 'by reasonable

security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.'

The GDPR incorporates this principle in its Article 32, demanding controllers and processors to take appropriate 'technical and organisational measures' when processing personal data. Such measures can include pseudonymisation or encryption, measures to ensure confidentiality of processing, or ability to recover data or restore processing in the event of system breakdown or malfunction in the course of processing.

In Ghana, Article 28(1) of the Ghanaian Act provides an almost identical security requirement as to Article 32 of the GDPR, also suggesting pseudonymisation and encryption as potential tools to ensure data security. This is equally the case in Kenya, as illustrated in the provisions of Article 41(4) of the Kenyan Data Protection Act.

4.5 Openness Principle (Paragraph 12 OECD Revised Guidelines)

Article 12 of the OECD Guidelines advocates 'a general policy of openness about developments, practices and policies with respect to personal data.' This is a very crucial data protection principle, and is geared towards establishing trust between individual and organisations which process their personal information. As de Hert et al. [21] observe, once an individual relinquishes their data, they are excluded from the processing, and have no say in how such processing may affect them in future e.g. as regards automatic inferences [21]. This principle flows from one of the main objectives of data protection legislation, namely making the data subject a participant in the outcome of their own data processing. It compels controllers to provide individuals with sufficient information on the processing being carried out, empowering them to scrutinize processing of their data through exercising rights like the right of access, modification and/or deletion of their information being processed [22].

In the GDPR, this principle is materialised in Article 5(a) as the 'transparency' principle, and is reflected in a number of obligations imposed on the data controller. For one, the controller is required to clearly inform data subjects the reason for which they are collecting and processing their information (Article 12(1)), especially when such processing requires (informed) consent from the data subject. The data controller also has to inform the data subjects of their rights to withdraw their consent at any later time if they so wish (Article 7 (1) to (3)). In terms of rights under this principle, Article 13(2)(f) notably grants data subjects the right to request that the data controller explains to them how a particular processing activity yielded a given result which affects the data subject. This right could be activated especially in cases where such decision was reached through automation i.e. with little or no human intervention in the processing.

In Ghana, Article 17(f) mentions 'openness' as one of the principles of data processing. Further consolidating this principle, Article 18 requires that the controller processes personal data lawfully and without violating individuals' privacy rights. Article 27(2) lists a relatively rather exhaustive list of information which the controller, before collecting data for processing, must ensure the data subject is aware of. These include, inter alia, the contact details of the data controller, the purpose for collection, legal grounds for the processing, whether there are or will be any third party recipients of the data, the data subject's right of access and, if need be, to request rectification of the collected and processed data. Moreover, the Act requires that when a decision which significantly

affects an individual is taken by automated processing, the data controller should notify the individual, hence providing an opportunity for objection (Article 41). Unlike in the GDPR however, there is no express right available for the individual to obtain meaningful information about the logic involved in processing their data.

The Kenyan Data Protection Act on its part guarantees this principle in its Article 25(b), requiring processing transparency on the part of the data controller. He is equally required in Article 29 to inform the individual about, inter alia, their rights with regard to processing, the purpose of processing as well as the contact details of the data controller or any third party who will receive the data as part of the processing procedure. While Article 32(1) places a burden of proof on the controller to prove consent for processing. In terms of data subject rights, Article 26(a) grants a right for data subject to be informed of the use for which their data is processed. This right proves useful for regulating further unauthorised processing by the controller, hence complementing the Purpose and Use Limitation principles. It should be noted however that just like with the Ghanaian Act, the Kenyan legislation appears offer no express right to data subjects to obtain an explanation from the data controller on the logic involved in processing.

4.6 Individual Participation Principle (Paragraph 13 OECD Revised Guidelines)

Paragraph 13 of the OECD Guidelines recommends that individuals should have the right to 'to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; to have [the data] communicated to them…in a form that is readily intelligible to them' and 'to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended.' This principle falls line with the somewhat supervisory role data protection law seeks to grant individuals over the processing of their information.

Accordingly, the GDPR grants a list of rights to data subjects from Article 15 to 18. Article 15 guarantees a right of access to personal data, which in essence gives individuals the right to 'obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information inter alia: the purposes of the processing, categories of personal data being processed, third party recipients if any, storage period of the data, right to restrict processing, or the right to lodge a complaint with a data protection supervisory authority'[15].

Article 16 complements the right of access with a right to rectification of inaccurate data. A right to erasure (also referred to as a right to be forgotten) is introduced in Article 17, which permits the data subject to request the data controller to erase all personal data it may have about them if, inter alia, processing is no longer compatible with the purpose of processing, they have withdrawn consent to the processing, or their

[15] Ideally, a data protection supervisory authority is an independent public authority in charge of overseeing compliance with data protection principles in a given jurisdiction. The GDPR's Article 51 requires each EU Member state to create at least one within each territory. In Ghana, the role is fulfilled by the Data Protection Commission, created by Article 1 of the Data Protection Act. In Kenya, the 2019 Data Protection Act 2019 establishes the Office of the Data Protection Commissioner in its Article 5.

fundamental rights override the processor's legitimate interest for processing. However, this right has to be balanced with other fundamental rights listed in Article 17(3) like freedom of speech and expression or general public interest (especially if the data subject is a public personality[16]). Article 18 then consolidates a right to request restriction of processing if, inter alia, the data is no longer accurate or needed for the purpose for which it was collected. Equally related to this principle is the right to data portability introduced by the GDPR's Article 20, which is a rather peculiar right in terms of granting control over personal data. The right permits data subjects to request their data under processing by a data controller to be transferred to another controller, where such data is processed by automated means.

In Ghana, Article 17(h) of the Ghana Data Protection Act notably mentions 'data subject participation' as a personal data processing principle, while Articles 32 and 35 list a relatively exhaustive set of provisions cumulatively arranged into 18 subsections relating to the right of access to personal data. It equally confers to data subject a list of rights similar to Article 15 of the GDPR, adding, inter alia, the need for consent of any other person who may be identified from the requested data or the data controller taking measures to de-identify them (Articles 35 (4) and (7)). Article 33(1)(a) confers a right to data rectification for individuals, while Article 33(1)(b) grants a 'right to be forgotten' similar to the GDPR. However, unlike the GDPR, there is no express right to data portability in the Ghana Data Protection Act.

In Kenya, similar to the Data Quality Principle, Article 26 (d) and (e) and Article 40(1) of the Kenyan Data Protection Act grant individuals a right to request the correction and deletion of false or misleading data about them. Article 34 grants rights on restriction of processing very identical to those listed under Article18 of the GDPR, and Article 36 provides a general right for individuals to object to processing unless the data controller proves legitimate interest which overrides the individual's interest. And, as in the GDPR, the Kenyan Data Protection Act provides for a right to data portability (Article 38). However, the Act does not appear to limit the right to data processed by automatic means. Apparently therefore, all forms of personal data, as long as they are structured and in a usable format, can be subject to the right to data portability.

4.7 The Accountability Principle and the Implementing Accountability Principle (Paragraphs 14 and 15 (B), OECD Revised Guidelines)

Paragraph 14 of the OECD Revised Guidelines makes data controllers responsible for giving effect to the principles advanced in the Guidelines. Complementing this positon, Paragraph 15 requires that they be prepared to show, upon request, a privacy management programme giving effect to the Guidelines. In essence, the Accountability Principle requires data controllers to always be in a position to demonstrate compliance with data processing requirements. It could be viewed as a supervisory mechanism to ensure that individuals are always guaranteed their data protection rights. The Implementing Accountability Principle follows up on this by requiring data controllers to always be poised to demonstrate at any time that they are compliant with data protection obligations.

[16] See Paragraph 99 of the ECJ's decision in Google Spain SL, Google Inc v Agencia Española de Protección de Datos and Mario Costeja González [2014] ECLI:EU:C:2014:317.

Incorporating this principle, the GDPR's Article 5(2) provides that the data controller 'shall be responsible for and be able to demonstrate compliance' with all the above data-processing principles. Article 25 on its part requires data controllers to construct their data processing activities in avid awareness of the data protection principles of the Regulation i.e. the conception and running of data processing activities should revolve around data protection principles (Data protection by Design or by Default). Moreover, a 'Data Protection Impact Assessment' requirement (Article 35 GDPR) obliges data controllers, where processing may be risky due to the nature of the data processed (like sensitive data), to carry out an assessment to clearly identify the dangers and risks such processing could present to data subjects. If risks are imminent, the processing could be ordered to stop (by the supervisory authority) or may be permitted to continue after a verified adoption of appropriate countermeasures.

The Ghanaian Data Protection Act mentions the term 'accountability' (Article 17(a)) as a principle to ensure the privacy of individuals but unlike the GDPR, it is silent as regards the data controller's use of default compliance mechanisms i.e. no express data protection by design requirement. There also appears to be no express obligation on data controllers to carry out a prior impact assessment (in the event of risky processing): rather, the Act only grants 'affected' individuals the possibility to request the Data Protection Commission to make such an assessment on a data controller's processing activity (Article 77). The Kenyan Data Protection Act on its part does provide for a 'Data protection by Default or by Design' requirement (Article 41), as well as a data protection impact assessment (Article 31).

4.8 Security Breach Notification (Paragraph 15(C), Implementing Accountability, Revised OECD Guidelines)

Paragraph 15 (c) of the Revised OECD Guidelines requires data controllers, as a measure to implement the Accountability Principle, to 'provide notice…to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data.' Apparently complementing the Security Safeguard Principle, this Principle was introduced in the 2013 Revised OECD Guidelines. It is worth mentioning that by the time of this revision, data breach notification requirements were already being implemented in a handful of countries and had been introduced in the US by the state of California in 2002 [23]. Data breach notifications have been asserted to serve three purposes: providing feedback on the strengths and shortcomings of a given security measures; enabling authorities and data subjects assess the data controllers's or processors' level of security with respect to their data processing activity; and they compel data controllers and processors to assess and understand their own security measures[17].

This Principle is materialised in the GDPR's Articles 33 and 34. Article 33 demands the data controller to record and/or report personal data breaches[18] to their data supervisory authorities, depending on the severity of the breach. Article 33(5) also compels data

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

[18] A personal data breach is defined by Article 4(12) of the GDPR as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

controllers to document or record the details of any eventual breach, its effects and the remedial action taken, and the documentation shall enable the supervisory authority to verify compliance with this Article. Article 34 requires that data subjects be informed in case of the breach is likely to affect them significantly, but then avails the data controller of this requirement if it had applied, on the breached data, relevant measures to render the data unintelligible (like encryption), or has taken other relevant measures to ensure that the breach does not materialise into a risk for data subjects.

In Ghana, Article 31 of the Data Protection Act requires the data controller, in event of a reasonable suspicion of a security compromise, to inform the Data Protection Commissioner and the data subject. The Act, however, does not adopt a risk-mitigating approach like the GDPR: not only does it require the reporting of mere suspicions of security compromises, it appears *all* security incidents must be reported, whether or not they are significant or the controller had encrypted the data or adopted other pre or post-mitigating measures. Contrarily, in Kenya, Article 43(1) requires notification if a breach[19] presents a 'real risk of harm' to the data subject. And just like the GDPR, it adopts a risk-mitigation approach by availing the controller or processor of the duty to notify the data subject if the latter took appropriate safeguards like encryption. A slight difference with the GDPR here though is that apparently nothing avails the data controller from notifying the Data Protection Commissioner despite adopting such post-breach mitigating measures (Article 43(6)). But then Article 43(8), just like the GDPR, requires the data controller to record the details of [every] personal data breach, its effect and the remedial actions taken.

5 Conclusive Remarks

This paper set out to review how the Ghanaian and Kenyan data protection legislations fare before the European GDPR in consolidating a right to personal data protection for their citizens; rights embedded in the OECD Revised Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 11th July 2013. First, it presented an overview of the importance of data protection as a legal regime and an essential, complementary safeguard against the fundamental rights and freedoms of individuals in today's world of ubiquitous computer and IT processing of personal information. It then briefly reviews the emergence of the 1980 OECD Guidelines (and later its revision in 2013) which laid down the essential principles of the right to data protection around which related national or supranational legislations around the globe could be developed. With the EU as well as African states like Ghana and Kenya adopting data protection legislations based on these OECD principles, this paper sought to comparatively examine the rights and obligations they confer respectively on individuals and data controllers within their jurisdiction. In this light, the incorporation of the OECD data protection principles in the GDPR was comparatively measured against the incorporation of the same principles in the Ghana Data Protection Act of 2012 and the Kenyan Data Protection Act of 2019.

[19] Article 2 of the Kenyan Data Protection Act adopts exactly the same definition of a personal data breach as Article 4(12) of the GDPR.

Compared to the European model, the Ghanaian and Kenyan data protection instruments have made quite commendable effort to consolidate the OECD data protection principles to their respective citizens. It can however be affirmed that the African legislations copied hugely from the European model's implementation of the OECD Principles; which can be understood from a viewpoint of colonial history as well as the desire to comply with European data protection standards for economic reasons. As has been commented [24], African data protection legislations are generally heavily influenced by European legislation, owing to colonial heritage as well as the desire to comply with the EU adequacy principle or the so-called 'Brussels effect'. Nevertheless, the Ghanaian Data Protection Act differs slightly from the GDPR and even the Kenyan Data Protection Act in the application of some of these Principles, as evidenced in the absence of a right to data portability, of an obligation to record a personal data breach, or no express requirement on the data controller to do a prior data protection impact assessment (the data subject has to seize the Data Protection Commissioner so the latter seizes the data controller to request n impact assessment). Another noticeable difference is its apparent 'laissez faire' latitude to data controllers to subject data subjects to decisions of purely automated systems unless the data subject expressly notifies the data controller not to refrain from doing so. This which could be problematic because, practically, as Africa and Ghana rapidly advance towards an Internet of Things, individuals would never be able to keep track of or even know about all the data they generate, much less the data a given data controller has about them and is ready to process for profiling and other profit-making purposes. The Kenyan Data Protection Act equally embeds all the above-selected OECD Revised Principles relating to rights and duties of individuals and data subjects respectively, literally copying Europe's GDPR for the most part.

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. Solove, D.: 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 (2008)
2. Xavier, C., Bosua, R., Maynard, S.B., Ahmad, A.: The Internet of Things (IoT) and its impact on individual privacy: an Australian perspective. Comput. Law Secur. Rev. **32**(1), 4–15 (2016)
3. González Fuster, G.: The emergence of personal data protection as a fundamental right of the EU. LGTS, vol. 16. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05023-2
4. Nam, T.: What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. Soc. Sci. J. **56**, 530–544 (2018)
5. Lynskey, O.: The Foundations of EU Data Protection Law. Oxford University Press, Oxford (2015)
6. Bennett, C.J.: Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Cornell University Press, New York (1992)
7. 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)

8. Greenleaf, G.: Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 45. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035. Accessed 11 Oct 2019
9. Bignami, F.: The case for tolerant constitutional patriotism: the right to privacy before the european courts. Cornell Int. Law. J. **41**, 211 (2008)
10. 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?. Springer, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_1
11. Solove, D.: The Digital Person: Technology and Privacy in the Information Age, vol. 1. NyU Press, New York (2004)
12. Arzt, C.: Data protection versus Fourth Amendment privacy: a new approach towards police search and seizure. Crim. Law Forum **16**(3), 183–230 (2005). https://doi.org/10.1007/s10609-005-4143-9
13. Solove, D.: Why I Love the GDPR: 10 Reasons. https://teachprivacy.com/why-i-love-the gdpr/. Accessed 11 Oct 2019
14. Dagbanja, D.N.: The right to privacy and data protection in Ghana. In: Makulilo, A.B. (ed.) African Data Privacy Laws. LGTS, vol. 33, pp. 229–248. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47317-8_10
15. Omane Boamah, E.K.: Minister for Communications at The Launch Of The Data Protection Commission On 18th November 2014 at The International Conference Centre (Data Protection Commission). https://dataprotection.org.gh/resources/downloads/conference/10-final-speech-of-the-hon-minister-of-communications-at-the-launch-of-the-data-protection-act/file. Accessed 11 Oct 2019
16. Agyei-Bekoe, E.: Empirical Investigation of the Role of Privacy and Data Protection in the Implementation of Electronic Government in Ghana. A Doctoral Thesis Submitted in Partial Fulfilment of the Award of Doctor of Philosophy Faculty of Technology, Centre for Computing and Social Responsibility De Montfort University, September 2013
17. Makulilo, A.B., Boshe, P.: Data protection in Kenya. In: Makulilo, A.B. (ed.) African Data Privacy Laws. LGTS, vol. 33, pp. 317–335. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47317-8_15
18. Pangrazio, L., Selwyn, N.: Personal data literacies': a critical literacies approach to enhancing understandings of personal digital data. New Media Soc. **21**(2), 419–437 (2019)
19. Fuster, G.G.: Inaccuracy as a privacy-enhancing tool. Ethics Inf. Technol. **12**(1), 87–95 (2010)
20. Wachter, S., Brent M.: A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Columbia Business Law Review (2019)
21. De Hert, P., Papakonstantinou, V., Wright, D., Gutwirth S.: The proposed Regulation and the construction of a principles-driven system for individual data protection. Innovation: Euro. J. Soc. Sci. Res. **26**(1–2), 133–144 (2013)
22. Coudert, F.: Towards a new generation of CCTV networks: erosion of data protection safeguards?. Comput. Law Secur. Rev. **25**(2), 145–154 (2009)
23. Stevens, G.M.: Data security breach notification laws. CRS Report for Congress (2012). http://dev.journalistsresource.org/wp-content/uploads/2012/04/R42475.pdf. Accessed 13 10 2019
24. Makulilo, Alex B.: "One size fits all": does Europe impose its data protection regime on Africa? Datenschutz und Datensicherheit-DuD **37**(7), 447–451 (2013)