Alma Mater Studiorum – Università di Bologna
in partnership with LAST-JD Consoritum:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in
Law, Science and Technology

**Cycle XXXII**

Settore Concorsuale di afferenza: 12H3
Settore Scientifico disciplinare: IUS20

TITLE OF THE THESIS

# ANALYSES OF SELECTED LEGAL ISSUES RELATED TO PERSONAL DATA SECURITY AND THE INTER-RELATIONSHIP BETWEEN PERSONAL DATA PROTECTION LAW IN AFRICA AND EUROPE

Submitted by: Alunge Nnangsope Rogers Alunge

The PhD Programme Coordinator
Prof.ssa Monica Palmirani

Supervisor
Prof. Massimo Durante

Co-supervisor
Prof. Michele Graziadei

Year 2020

Alma Mater Studiorum – Università di Bologna
In collaborazione con LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

DOTTORATO DI RICERCA IN

Erasmus Mundus Joint International Doctoral Degree in
Law, Science and Technology

**Ciclo XXXII – A.A. 2016/2017**

Settore Concorsuale: 12H3
Settore Scientifico Disciplinare: IUS20

TITOLO TESI

# ANALYSES OF SELECTED LEGAL ISSUES RELATED TO PERSONAL DATA SECURITY AND THE INTER-RELATIONSHIP BETWEEN PERSONAL DATA PROTECTION LAW IN AFRICA AND EUROPE

Presentata da: Alunge Nnangsope Rogers Alunge

Coordinatore Dottorato
Prof.ssa Monica Palmirani

Supervisore
Prof. Massimo Durante

Co-Supervisore
Prof. Michele Graziadei

Esame finale anno 2020

## Abstract

It has been well documented that the unprecedented and increased use of computerized technology to process personal information in the 1960s in Europe and the US led to concerns about individual privacy, which resulted in the introduction of a branch of law regulating the processing of personal data, known today as personal data protection law. Over the years though, not only has its principles evolved to include processing of non-digital information, this relatively new domain of law has introduced informational rights and obligations which appear to have the capacity to regulate a vast variety of domains of activity in as much as they involve collecting and processing information about humans. This publication-based thesis regroups five published/accepted articles which generally seek to appreciate the significance of rights and obligations of this branch of law within the EU and Africa, while identifying the differences between both jurisdictions and exploring the impact of EU data protection law on its contemporary African counterpart.

The Chapters in this thesis focus on a limited variety of selected themes in data protection law. The first Chapter addresses the lack of clarification of the meaning of a breach of security in EU data protection law, and the second Chapter examines the level of personal data security protection guaranteed by African regional data protection instruments in comparison with the current European data protection regime. The third and fourth Chapters both explore the potential effect of the transposition of EU data protection legal standards into African soil, respectively focusing on the processing of public examination results and on curtailing the prevalence of teacher-student abuses on university campuses. The fifth and final Chapter presents a comparative analysis between the EU GDPR, the Ghanaian Data Protection Act 2012 and Kenyan Data Protection Act 2019 in their approaches to consolidate the OECD data protection principles, demonstrating the influence of the GDPR on the Kenyan Act as opposed to that of Ghana. The thesis conclusively finds that transposing EU data protection standards into Africa could help regulate some under-regulated domains of activity. But the continent's institutions still need to do a lot in terms of harmonising and promoting personal data protection law among its countries.

**Acknowledgments**

Heartfelt gratitude to my supervisors Professors Massimo Durante and Mcihèle Graziadei for their unrivaled support, guidance, openness and patience in following up the progress of this work throughout this PhD program.

Also wish to thank fellow colleague Urbano Reviglio for his constant feedback on my manuscripts and interdisciplinary advice which contributed immensely to the final output herein.

Sincere thanks to Professor Monica Palmirani and Dr Dina Ferrari for the technical and administrative support to ensure a comfortable stay for me in Italy and the overall smooth-running of the LAST-JD PhD Programme.

**List of abbreviations**

ACHPR…….African Charter on Human and People's Rights

AU…….African Union

CFR……Charter of Fundamental Rights of the European Union

CoE…….……..Council of Europe

ECHR…….……..……European Convention on Human Rights

ECJ…….……European Court of Justice

ECOWAS……..……Economic Community of West African States

EDPS…….European Data Protection Supervisor

EU……..…European Union

GCE…….…….General Certificate of Education

GDPR ……..……..…….……General Data Protection Regulation

NIS……Network and Information Security

OECD……Organisation for Economic Cooperation and Development

WAEC…….……West African Examination Committzz

WP29……..…….EU Article 29 Working Party

# Table of Contents

## General Introduction

This general introduction presents the general background, methodology, structure, and scope of the thesis. It provides information on the objectives of the research questions, the purpose and rationale of the study, and describes the research and data collection methods employed. It also presents an overall summary of the publications regrouped in the thesis.

## Background of the thesis

### The (emergence of the) Right to Personal Data Protection

The origins of the right to personal data protection lie partially in the data protection rules of northern European countries, which arose in several nations in the 1970s, and the Council of Europe's Resolutions on data processing and partially in the USA and the realization of so called Fair Information Practices (FIPs), which were developed because the right to privacy was thought to be unfit for the 'modern' challenges of large automated data processing.[1] By the beginning of the 1960s, computers were already being depicted as a major threat to the privacy due to their ability to easily and inexpensively process massive amounts of information and hence governments' ability to store massive amounts of information about their people.[2] This scale of vast, automated processing made it increasingly difficult to protect the traditional right to privacy[3], raising the need for a novel set of rules to control automated processing of personal information.

In response to this development, the US Department of Health, Education and Welfare conceived a set of principles referred to as a Federal Code of Fair Information Practices (FIP) in 1973. It incorporated five core principles as follows:

- There must be no personal data record-keeping systems whose very existence is secret.

[1] Bart Van der Sloot. "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?" In *Data protection and privacy:(in) visibilities and infrastructures*, pp. 3-30. Springer, Cham, 2017.3

[2] Alan Westin. *Privacy and Freedom*. (Originally published in 1967). Ig Publishing. 2015 (e-book). 209

[3] Privacy in this context refers to informational privacy, which Westin defines as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (Alan Westin. *Privacy and Freedom* (2015) ibid, 23). It should be mentioned that today, the word "privacy" is currently used to describe a myriad of different things: freedom of thought, control over personal information, freedom from surveillance, protection of one's reputation, protection from invasions into one's home, the ability to prevent disclosure of facts about oneself…" (Daniel Solove. "Conceptualizing privacy." *Calif. L. Rev.* 90 (2002): 1096). The earliest mention of "privacy" as a distinct legal concept can be traced back to the late 19th Century, in the essay titled "The Right to Privacy" by Judge Samuel Warren and Louis Brandeis in 1890 [3], in which they defined the right to privacy as the right of an individual to "be let alone". The right was later embedded by the United Nations in Article 12 of the Declaration of Human Rights of 10th December 1948, prohibiting arbitrary interference with the 'privacy, family, home or correspondence' of a person, or 'attacks upon his honour and reputation'.

- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[4]

These principles, in essence, aim at protecting individuals by giving them some form of control over information processed by government agencies, and form an essential part of the normative core from which is developed contemporary personal data protection law. Or in other words, they lay a partial foundation for the contemporary right to personal data protection.

Within the European Community, data protection as a (fundamental) right can be traced from the adoption of the European Charter of Human Rights (ECHR) in 1950 by the Council of Europe as a European adaptation to the UN General Assembly's Universal Declaration of Human Rights of 1948, consolidating a right to privacy in its Article 8, as follows: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' It has been pointed out that this right to privacy, like the entire European Charter and UN Declaration, came about as a means to curtail the powers of abusive totalitarian states before and during the just ended Second World War,[5] and was aimed at protecting individuals from interference by the state into their private life. Apparently in an attempt to ensure compatibility of the right with the rising use of ICTs in human correspondences, the European Court of Human Rights adopted a generally broad approach to the notion of 'private life', extending it far beyond the intimate sphere of the physical home, and even bringing in telephone conversations computers, video-surveillance, voice-recording and Internet and e-mails under the coverage of Article 8[6]. However, by the early 1970s and just as was the case in the US as discussed above, the Council of Europe concluded that Article 8 ECHR suffered from number of limitations in

[4]U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (Washington, D.C.: 1973), p.41

[5] Bart van der Sloot. "Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR." In *Group Privacy*, pp. 197-224. Springer, Cham, 2017.200. Also see Bart van der Sloot. *Privacy as virtue*. Intersentia, 2017. pp. 23-24.

[6] Paul de Hert and Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." (2009) supra,.16

the light of new developments, particularly considering new developments in the area of information technology[7]. In a report by the Committee of Ministers in the 1960s on whether the ECHR gave sufficient protection to the right to privacy in view of developments in information processing, the Committee pointed out three main problems. First, Article 8 was targeted against state interference on the individual, and did not consider or apply to interference by elements of the private sector. Actually, as per Article 35 of the ECHR, complaints based on the Charter against elements of the private sector were not admissible before the European Court of Human Rights (ECtHR) for lack of *rationae personae* jurisdiction; only state institutions could be sued before the Court under the Charter. Secondly, the right to private life under Article 8 ECHR does not cover all forms of personal information, which leaves a large category of unprotected information (an example being *identifiable* information). Thirdly, the right of access to information about one's self is not covered under Article 8 ECHR.[8]

Following this report, efforts were made at national level to adopt laws regulating the processing of personal information by the early 1970s, beginning notably with Sweden[9] and Germany[10]. Later, following recommendations by the Council of Ministers, Convention 108[11] protecting individuals with regard to the processing of their personal data was adopted by the Council of Europe on 28th January 1981. This period also witnessed a landmark reasoning by the German Constitutional Court (Bundesverfassungsgerichsthof) in its decision of 15th December 1983[12], also referred to as the Population Census Decision[13] considered to be one of the normative foundations of contemporary data protection law in Europe. The Court established a right of every citizen to 'information self-determination', founded on the right to the 'free development of one's personality' (or personality right) as protected by Article 2.1 of the German Constitution. In essence, just as the internationally recognized right to self-determination protects an individual's right to plan or decide freely without

[7]Peter Hustinx. "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* (2013): 1-12.4

[8] See Paul de Hert and Eric Schreuders. "The relevance of Convention 108." Published in: *European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future*. 2001.

[9] Swedish Datalag (Data Act) of 11 may 1973

[10] Gesetz zum Schutz vor mißbrauch personenbezogener Daten bei der Datenverarbeitung (Law on protection against the misuse of personal data in data processing) (Bundesdatenschutzgesetz—BDSG) (Federal Data Protection Act) of 27 January 1977, Bundesgesetzblatt (BGBl)

[11] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.

[12] Judgment of 15 December 1983, 1 BvR 209/83, BVerfG 65, 1

[13] Orla Lynskey. *The foundations of EU data protection law*. Oxford University Press, 2015. 94

being subject to pressure or influence, the right to information self-determination aims to 'preclude a social order in which citizens no longer can know who knows what, when, and on what occasion about them.'[14] If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, or know who may have access to this information, or unsure of whether their dissenting behaviour is noticed or stored, they may be inhibited in exercising their fundamental human rights like freedom of speech or choice[15]. A decade later, the EU Commission adopted the Data Protection Directive of 1995,[16] with the objective to 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' (Article 1(1)), reflecting the Council of Europe's Convention 108 and further consolidating the above position of the German Constitutional Court into EU law. Five years later, the right to data protection officially attained the status of a fundamental right in the European Union, embedded in Article 8 of the EU Charter of Fundamental Rights of 7th December 2000. Then came the General Data Protection Regulation (GDPR),[17] replacing the 1995 Directive and establishing harmonised personal data protection rules directly applicable to all EU member states.

For purposes of conceptual clarity, this thesis shall formulate and adopt a definition of personal data protection based on the 2013 analysis of the above Convention 108 and the 1995 Directive by the then European Data Protection Supervisor, Peter Hustinx. He interpreted the concept as referring to those set of rules and safeguards to be observed when processing personal data in order to protect the fundamental rights and freedoms of individuals (including privacy) from any eventual violation.[18]

**Extraterritoriality of EU (data protection) law**

Legal scholars have shed light on how the EU has been increasingly confident to influence external regulatory spaces.[19] Despite being overshadowed on the international economic and military scene by

[14] Antoinette Rouvroy & Yves Poullet. "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy." In *Reinventing data protection?*, pp. 45-76. Springer, Dordrecht, 2009. 49

[15] Gerrit Hornung & Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25, no. 1 (2009): 84-88. 85

[16] 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.

[17] 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

[18]Peter Hustinx. "EU data protection law" (2013) supra 1-12.

[19] For a discussion on the extraterritorial effects of EU standards, see Joanne Scott. "Extraterritoriality and territorial extension in EU law." *The American Journal of Comparative Law* 62, no. 1 (2014): 87-126; Anu Bradford. "The Brussels Effect' (2012)." Northwestern University Law Review 107 (2012): 1; Maria O'Neill. "The Legal Reach of Police and

the US and Asia, Europe still wields a rather underestimated influence on global standards.[20] In the last decades, standards set by EU institutions in various domains are increasingly being regarded around the globe as the standards to comply with, leading to what Bradford terms "unilateral regulatory globalization" which occurs when a state is able to externalize its regulations outside its borders through market mechanisms, resulting in the globalization of its standards.[21] Or where a law of one jurisdiction migrates into another in the absence of the former actively imposing it or the latter willingly adopting it.[22] Bradford observes that the EU manages to do this due to its imposing market size [with 500 million consumers and a GDP of over 20 trillion USD by 2017[23]], capacity to impose significant costs on noncompliant external entities by excluding them from their market, and capacity to maintain strict regulatory standards on its consumer markets, taking advantage of their inelasticity.[24] As a result, foreign business agents wishing to be part of the EU market must either comply with EU standards or, as shall be discussed further in Chapters 3, 4 and 5 of this thesis, foreign states may decide to ease access to EU markets by internalising similar EU standards. It therefore turns out that the EU effort to create a European single market, has led to a probably unintentional effect of establishing the EU as a global regulatory hegemon,[25] which Bradford terms the "Brussels Effect".[26]

In the same light, Scott asserts the emergence of the image of an EU that is "unilateralist, hegemonic and where the direction of regulatory travel is all one way, namely from the EU to the rest of the world."[27] She notably argues that the EU makes use of a mechanism she terms "territorial extension", which she defines as "the application of a measure triggered by a territorial connection but in applying the measure the regulator is required, as a matter of law, to take into account conduct or

---

Judicial Co-operation in Criminal Matters (PJCCM) Measures across EU Borders: Extraterritoriality, Territorial Extension and the "Brussels Effect". In *EU Borders and Shifting Internal Security*, pp. 139-156. Springer, Cham, 2016.

[20]See Anu Bradford. "The Brussels Effect." (2012) ibid: 1

[21] Ibid, 3. Bradford further points out that unilateral regulatory globalization is different from "political globalization of regulatory standards" where regulatory convergence results from negotiated standards, including international treaties or agreements among states or regulatory authorities; and also from "unilateral coercion", where one jurisdiction imposes its rules on others through threats or sanctions.

[22] Ibid, 4

[23] *European Union*, CIA WORLD FACTBOOK, https://www.cia.gov/library/publications/the-worldfactbook/geos/ee.html (Accessed 7th May, 2020)

[24] Anu Bradford. "The Brussels Effect." (2012) supra. 11 – 17. He also notes that unlike capital targets (i.e. goods used for production) which can be relocated from the EU if found unsatisfactory for businesses, the consumer market remains mostly inelastic. Which is why the EU focuses its regulation on consumer goods, because its consumer population cannot be relocated elsewhere to be subject to less strict standards.

[25] Ibid, 42.

[26] Ibid, 3

[27] Joanne Scott "Extraterritoriality and territorial extension in EU law." (2014). supra. 88

circumstances abroad"[28] The EU sets standards across a range of areas, such as food, competition, and even privacy and data protection, which then dictate how other states or regions end up regulating these sectors as they adjust their own regulatory standards in order to access the EU consumer market. This effect is reflected in the influence of EU data protection law across the globe, and significantly on African jurisdictions.

**Euro-African legal "compatibility"**

Long before the creation of the EU, Africa had already been largely affected by European standards owing to its colonial relationship with European powers during the colonial era (between the 1880s and 1960s). During this period, a handful of European powers moved in and annexed African territories in their quest to establish overseas strongholds, with about 80% of the continent falling under the control of Britain and France after receiving German colonies following the latter's defeat during the First World War.[29] The European powers generally subjected the colonial officials administering their colonized territories to the laws of the mother state, before extending their application to the locals while abolishing customary law hitherto practiced by the natives towards the end of the colonial era.[30] After obtaining their independence in the 1960s and 1970s, many African nations decided to maintain the political and legal institutions left behind by their various former colonial masters, notably in the education, administration and legal justice sectors[31]. European law especially English common law introduced by England and *droit civil continental* (civil law) designed by continental European powers were therefore maintained by the newly independent African colonies, and most national laws and rules of procedure in these countries are still inspired from these legal systems and still operates in most territories to date.[32] Africa is therefore no stranger to European law, which favours the continent's ability to appropriate contemporary and future European (legal) standards.

---

[28] Ibid, 90. She also distinguishes territorial extension from traditional extraterritoriality, which is the application of a measure triggered by something other than a territorial connection with the regulating state

[29] Worldwide Perspectives GMMS 2007. 'The 25 Unbelievable Years: Colonial Africa in 1945' [Map]. Available at https://www.missioninfobank.org/mib/index.php?main_page=product_info&products_id=3576

[30]Alexander Lee & Kenneth A. Schultz. "Comparing British and French colonial legacies: A discontinuity analysis of Cameroon." In *APSA 2011 Annual Meeting Paper*. 2011.13

[31]For a discussion on the inheritance of the colonial systems of administration and legal justice law by independent African countries, see Sandra Fullerton Joireman. "Inherited legal systems and effective rule of law: Africa and the colonial legacy." *The Journal of Modern African Studies* 39, no. 4 (2001): 571-596.

[32] Joireman (ibid) points out that this inheritance also came about because African elites who received training in Europe became experts in these foreign legal systems, and were instrumental in using them to negotiate for the independence of African states. They therefore were more comfortable with the system and desired to see it continue. See Ibid, 577

**Scope of the thesis**

It is against the above background that this thesis addresses some selected legal issues related to personal data processing in Europe and Africa, while examining the current and potential appropriation of EU standards in African national and regional data protection law. The articles regrouped herein address personal data security law in Europe and Africa, and the substantive and potential influence of EU data protection law on its African counterparts. The thesis discusses, in terms of its scope, relevant regional European and African laws relating to personal data processing. For Europe, analysis are centred on the General Data Protection Regulation[33] the 1995 Data Protection Directive[34] as well as the Network and Information Security (NIS) Directive.[35] For Africa, selected legislations include the ECOWAS[36] Supplementary Act A/SA.1/01/10 Personal Data Protection within the ECOWAS of 16th February 2010, the African Union Convention on Cybersecurity and Personal Data Protection, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019. Specifically, the thesis chapters:

- attempt a critique of the definition of a personal data breach in EU data protection law in relation to the notification of data breaches to data subjects;
- examine the state of the art of the legal responses by the ECOWAS and AU Data Protection legislations to personal data security risks in Africa;
- discuss the potential effect of EU data protection law's appropriation of examination results as personal data on African jurisdictions,
- demonstrate how EU case law relating to the personal data protection right of access to examination scripts could have parallel effect in Africa and help curb teacher-student abuses in institutes of higher education;
- make a comparative analysis between the GDPR on the one hand and the Ghanaian and Kenyan data protection Acts on the other hand with regard to their incorporation of international data protection standards laid down by the OECD, demonstrating the influence of EU data protection law its African counterpart.

[33] 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)

[34] 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

[35] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[36] Economic Community of West African States

**Purpose of the study and approach**

The general purpose of the papers regrouped in this thesis is to explore and evaluate certain legal issues relating to personal data security in Europe and Africa, and also how the legal and ethical realities of both continents influence or could inspire each other in their various conceptions of personal data protection law. The results and conclusions in each of these articles is intended to contribute to general legal literature to the domain of personal data protection, and to assist legal scholars, lawyers, judges, business executives, governmental officials, and policy makers in deciding on best practices and areas of improvement in their conception, discussions and interpretations of personal data protection law.

As regards the approach used in the articles, they generally employed involved three classic levels of policy analysis: macro, mezzo, and micro. The macro level of analysis involved basing arguments on general theory and principles of international legal standards and generally accepted principles. The mezzo level involved analysis of data protection laws, policies, and practices in Europe and Africa. At micro level, certain specific areas of EU and African data protection law as were examined and/or compared. The conclusions and recommendations were based on an integration of all three levels of analysis. It should however be noted that considering the themes, chosen topics, conditions of publication and author guidelines of each of the journals and conferences in which the thesis articles were reviewed and accepted, these three levels of policy analysis are not uniform in all the articles. While some articles involved all three levels of analysis, others only involved analysis at mezzo and macro level.

**Objectives of the thesis and research questions**

As private organizations and governments keep manifesting insatiable appetite for data, trusting in its ability to inform decision-making through data analytics and render it more efficient, personal data protection law has steadily become a principal means to place checks and balances on the processing of personal information to avoid violation of an individuals' stemming from any misuse of or omissions in the processing activity. As discussed above, these checks and balances come in the form of rights and obligations for data subjects and data controllers or processors respectively. This thesis, through the article publications regrouped herein, generally seeks to appreciate the significance of rights and obligations under EU and African data protection law, while identifying the differences between both jurisdictions and discussing the current and potential impact of EU data protection law on its contemporary African counterpart. In doing so, it highlights and examines the notion of personal data security within the EU and Africa, the interplay between EU and African regional law on the notion personal data and the right of access to personal data, and also provides a comparative analysis between the substantive data protection texts of the EU and selected African states.

In detail, the aim of the thesis is two-fold. Firstly, on personal data security, it seeks to contribute to data protection literature by highlighting the limitations of the current definition of a personal data breach in EU law in relation to protecting data subjects through breach notification, while clarifying the conceptual difference between a personal data breach and a breach of security, and also by examining the state of the art of Africa's multilateral response to the personal data security concerns of the continent. While there has been a lot of literature on personal data breaches in EU data protection law[37], not so much has been dedicated to address the potential limitations of the definition of a personal data breach in EU texts. And while the ECOWAS and AU data protection legislations have been examined in a number of scholarly articles[38], there has been a significant lack in the literature focused specifically on their provisions and shortcomings relating to personal data security.

Secondly, the thesis strives to illustrate the potential effect of EU law on African data protection law first through the latter's adoption of the notion of personal data and its potential similar application to academic examination scripts and results as well as the socio-legal effects of these eventualities. There have indeed been scholarly works analyzing and mapping Africa's adoption of data protection laws,[39] but these works do not focus properly on the substantive interpretation of these laws and their socio-cultural or legal effect on Africans. This thesis seeks to fill this gap by illustrating the significance the notion of personal data in the African education sector, and how data protection rights can introduce unprecedented and novel means of protecting African students against big data risks and even help combat teacher-student abuse in African university campuses. Also, a comparative

[37] See Rebecca Wong. *Data security breaches and privacy in Europe*. Springer, 2013. Also Spencer Wheatley, Thomas Maillart & Didier Sornette. "The extreme risk of personal data breaches and the erosion of privacy." *The European Physical Journal B* 89, no. 1 (2016): 1-12.

[38] See Uchenna Jerome Orji. "Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act." *International Data Privacy Law* 7, no. 3 (2017): 179-189; "A Comparative Review of the ECOWAS Data Protection Act." *Computer Law Review International* 17, no. 4 (2016): 108-118; "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*, pp. 105-118. IEEE, 2015. Also see Graham Greenleaf & Marie Georges. "The African Union's Data Privacy Convention: A Major Step toward Global Consistency?" *131 Privacy Laws & Business International Report, 18-21* (2014). Also Lukman Adebisi Abdulrauf & Charles Manga Fombad. "The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?" *Journal of Media Law* 8, no. 1 (2016): 67-97.

[39] See Alex B. Makulilo, ed. *African data privacy laws*. Springer International Publishing, 2016; "Privacy and data protection in Africa: a state of the art." *International Data Privacy Law* 2, no. 3 (2012): 163-178. Also Cynthia Rich. "Privacy laws in Africa and the Middle East." *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA* (2014). Also Lee A. Bygrave."Privacy and data protection in an international perspective." *Scandinavian studies in law* 56, no. 8 (2010): 165-200.

analysis between the EU GDPR and the Ghanaian and Kenyan data protection laws on their consolidation of the OECD data protection principles seeks to provide a novel appraisal of the influence of the GDPR on national African data protection laws; in this case the Kenyan Data Protection Act of 2019.

These aims will be achieved by analyzing and attempting an interpretation of the relevant provisions relating to personal data protection and personal data security in the EU and Africa. Both the law (substantive texts) and its application (case law and practical outcome) will be closely examined as it is often the case when reading the legal rules of two regimes against each other to identify theoretical similarities and differences. Also, through publications which consider and compare EU data protection provisions against African data protection legislations, this thesis aims to make the essence of data protection law more digestible for African lawyers in light of its significance in protecting the fundamental rights of individuals through the spectrum of their personal information.

Accordingly this thesis poses the following general research questions: What is the state of the art of personal data security law in the EU and Africa? How can EU data protection law and practice influence African national and multilateral data protection regimes? These questions can be subdivided into five sub-questions, each corresponding to and addressed by one of the five articles regrouped in the thesis: What are the limitations in the current definition of a personal data breach in EU law with regard to its difference with a breach of security and the protection of data subjects through breach notification? What is the current state of the art of Africa's multilateral response to personal data security concerns in the continent? How can EU data protection law and practice lead to examination results be considered personal data in Africa, and what are the benefits and hindrances in implementing corresponding data protection rights on examination results within an African setting? Similarly, how can EU data protection law potentially influence the application of a data protection right of access to evaluated examination scripts in Cameroon universities, and how could this contribute to curtailing teacher-student abuses? What are, and how has the GDPR been instrumental in the differences between the 2012 Ghanaian Data Protection Act and 2019 Kenyan Data Protection Act in their consolidation of the OECD personal data processing guidelines?

**Rationale of the thesis**

The published articles regrouped in this thesis are particularly important for academic research, legal practitioners and policy makers working in the field of personal data protection. In their attempts to provide an answer to each of the research problems highlighted above, the articles contribute novel

layers of thought and analysis which could aid the understanding and promotion of the data protection machinery.

In terms of examining the limitations of the definition of a personal data breach, the thesis discusses the difference between a breach of security and a personal data breach, and argues that discarding, from the scope of the definition, security incidents which have not resulted in an obvious compromise of personal data limits protection for data subjects in terms of breach notification. By proposing an alternative definition to personal data breaches and suggesting an alternative approach to notifying data subjects of security incidents the thesis hopes to trigger a thought process among EU and other data protection scholars and professionals on how to further improve protection of data subjects. Also, with no current definition of a 'breach of security' in EU legal texts, and considering that EU law requires certain actions for personal data breaches different from actions for breaches of security, understanding this distinction becomes crucial for data controllers in terms of compliance.

On the question of the state of the art of personal data security in Africa, the thesis provides an analysis of the security provisions of the ECOWAS and AU data protection texts, pointing out their achievements and grey areas which they fail to cover. This analysis would be of particular interest to African data protection academics and regional policy makers, who could respectively initiate research and political mechanisms to address these legal loopholes. Such analysis is also beneficial in terms of setting an albeit "soft" legal threshold for African countries which do not yet have national data protection legislations and who will tend to look up to these legislations as a model to which data controllers in their respective territories could abide by.

The analysis of examination results as personal data in Africa, by highlighting a novel perspective to the influence of EU law and practice on African data protection law, contributes further to the literature on Euro-African relations. More importantly, it also raises awareness among African education policy makers on the hitherto neglected significance of exam results as personal information (which misuse could expose Africans to risks especially associated with big data analytics), and could influence a new phase in the regulation of their processing. Similarly, demonstrating that evaluated examination scripts could be personal data under the AU Data Protection Convention, and hence could benefit from a right of access which then presents a novel way of curtailing teacher-student abuse in university campuses is of particular importance to student unions or associations working on students' rights, as well as policy makers in the higher education sector in Cameroon and other African countries. Finally, the comparative analysis between the GDPR and the Ghanaian and Kenyan data protection Acts in their consolidation of the OECD data protection Guidelines adds to the general

literature on comparative (data protection) law. It also provides an opportunity for African states still to enact national data protection laws to better appreciate the privacy and risk-based approaches to data protection and hence adopt informed national policies (i.e. either of, or a hybrid of both approaches) based on their respective national priorities.

**Methodology and data collection**

Based on the nature of the objectives and subject matter of the articles in this thesis and the corresponding nature of the research questions, this research makes use of both the descriptive exploratory and comparative methods of research. In essence, apart from the first chapter on a breach of security, all the articles in this thesis employ a blend of all three research methods.

Descriptive methodology, also referred to as phenomenological methodology, refers to "how things appear, an observable fact, or to let things speak for themselves", characterized as bringing reflective awareness to the nature of events experienced in the world in which we live in, favouring a deeper understanding of the nature or meaning of everyday lifeworld experiences.[40] It favours an intensive examination to grasp a deeper meaning of a phenomenon, presenting a picture of specific details of a situation and focuses on reflection questions.[41] As regards the exploratory research method, Fouché and Vos note that this is undertaken when more information is needed concerning a new area of interest or when researchers want to understand a certain situation better.[42]

Comparative law can be defined as an 'intellectual activity with law as its object and comparison as its process'[43] or as 'the juxtaposing, contrasting and comparing of legal systems or parts thereof with the aim of finding similarities and differences.'[44] These definitions, although quite general, considerably satisfy the purposes of the last four articles presented in this thesis. Zweigert and Kotz argue that 'comparative law procures the gradual approximation of viewpoints, the abandonment of deadly complacency, and the relaxation of fixed dogma'[45] which is exactly what this thesis aims to achieve when it compares the EU and African data protection systems. And according to Orucu, comparative law enables 'access to legal knowledge which can be used not only for the purposes of

[40] Marsha Smith Blount. *A phenomenological analysis of artistic creativity—contemporary artists' practice and philosophy*. Stephen F. Austin State University, 2007.33

[41] Christa Fouché & A. S. De Vos. "Formal formulations." Research at grass roots: For the social sciences and human service professions 4 (2011): 89-100.96

[42] Ibid 106

[43] Hein Kotz & Konrad Zweigert. "Introduction to Comparative law." *Vol. II (T. Weir trans. 2ed 1987)* (1998).2

[44] Esin Orucu, 'Developing Comparative Law' in Esin Orucu and David Nelken (eds), *Comparative Law; A Handbook.* Hart Publishing (2007) 43, 44

[45] Hein Kotz & Konrad Zweigert. "Introduction to Comparative law." (1998) supra, 3

law reform, or as a research tool, or to promote international understanding, but to fulfil the essential task of furthering the universal knowledge and understanding of the phenomenon of law which is under examination'[46]

It should be highlighted that thesis features comparisons between African national and regional data protection instruments with the EU GDPR and 1995 Data Protection Directive all of which, presumably, may not be regarded as a traditional comparative study in the sense of comparing the legal systems of sovereign states. A legal system has been said to refer to 'the legal rules and institutions of a country in the narrow sense or, in the broad sense as the juristic philosophy and techniques shared by a number of nations with broadly similar legal systems.'[47]Being made up of countries with fundamentally similar but nevertheless different legal systems and practices, African regional legislations (the AU Data Protection Convention and ECOWAS Data Protection Act) and EU laws like the GDPR probably does not fall within the narrow definition of what a 'legal system' is. However, these international instruments represent an agreed move by 27 (EU), 15 (ECOWAS) and 55 (AU) states to comply with specific rules and regulations in terms of processing personal information; a fact which favours their consideration as (data protection) legal systems in their own right. Moreover, a legal system 'has a vocabulary used to express concepts, its rules are arranged into categories, it has techniques for expressing rules and interpreting them, it is linked to a view of the social order itself which determines the way in which the law is applied and shapes the very function of law in that society.'[48] The GDPR, ECOWAS and AU data protection instruments seemingly satisfy these requirements as they have as objective to shape the law governing personal data within their various communities. Their nature as non-traditional legal systems cannot be ignored but could simply be considered inconsequential to the achievements of the comparative exercise in the articles presented in this thesis. After all, comparative research is considered to be open-ended with no standard methodology[49], and as Reitz observes, no promising avenue [of improving our understanding of the impact of law on society through research] meliorating should be barred by orthodoxy.[50] On this basis, this thesis considers it convenient to carry out an exercise of comparative law between the GDPR, ECOWAS, AU instruments and national laws on personal data protection.

[46] Esin Orucu. 'Developing Comparative Law' (2007) supra, 46
[47] Peter de Cruz. *Comparative Law in a Changing World*. 3rd edition. Routledge Cavendish. (2007) 3.
[48] David and Brierly as quoted by Orucu, 'Developing Comparative Law' (supra) 57
[49] Orucu, 'Developing Comparative Law' supra, 48-49
[50] John Reitz, 'How to Do Comparative Law' 46 (4) AJCL (1998) 617, 618

Both descriptive and exploratory methods were employed in the first article of this thesis: the exploratory method was employed to clarify the meaning of a "breach of security" in the EU data protection law based on a descriptive analysis of its rules of secure processing and some relevant provisions of the EU Network and Information Security (NIS) Directive (NIS). The descriptive method was then employed to portray the limitations of the EU definition of a personal data breach in relation to notifying data subjects of potentially harmful incidents, leading to the suggestion of an alternative, information security-based approach. In the second article, the descriptive method was used to provide an explanation and understanding of personal data security risks and concerns in Africa and the corresponding legal responses by the AU and ECOWAS bodies. Comparative law was then used to measure these responses to the EU (and to an extent US) instruments addressing personal data security to point out the weaknesses of the former.

The third and fourth articles make use of all three research methods. In the third article, a descriptive analysis was employed to produce a general appraisal of the socio-cultural context of privacy and data protection in Africa with regard to examination results, and exploratory method was used to interpret the decision in Nowak v. Irish Commissioner as granting a personal data status to examination results. Comparative law was then employed to examine and highlight the similarity of the definitions of personal data in both African and EU regional data protection instruments, while further use of exploratory research led to the analysis founding the potential interpretation examination results as personal data under the African data protection instruments. Similarly, the fourth article described the contemporary situation of teacher-student abuse in Cameroonian universities, before relying on comparative law and exploratory research to conclude that examination script evaluations could take up a personal data status in Cameroon upon the entry into force of the AU Data Protection Convention, and explain how this could help fight against teacher-student abuse. The fifth article takes a pure comparative law approach to directly compare, on the one hand, the GDPR's materialization of the OECD personal data processing guidelines with that of the Ghanaian and Kenyan data protection laws on the other hand, identifying the similarities and differences between the EU instrument and African national legislations. All the while demonstrating, in the process, the GDPR's influence on the Kenyan data protection Act.

Data analysed in the various articles in this thesis were collected from primary and secondary sources. Primary data sources of legal research have been said to refer to data produced by the legal process itself, including legislations and case law, while secondary sources include documents which

interpret and discuss the primary sources.[51] For this thesis primary sources include European data protection and security instruments in Europe, Africa and the OECD. The sources in Europe include the Council of Europe's Convention 108 on the automatic processing of personal data, the EU 1995 Data Protection Directive, GDPR, and the NIS Directive. African instruments include the 2010 AU Convention on Cybersecurity and Data Protection 2014, the 2010 ECOWAS Data Protection Act, the 2012 Ghanaian Data Protection Act and the 2019 Kenyan Data Protection Act. For the OECD, primary data was collected from the 1980 OECD Privacy Guidelines (Revised in 2013). Secondary data on the other hand was obtained from books, articles and handbooks by legal scholars interpreting and analyzing the above primary sources or providing more insight on personal data protection law and information security in general. Data was also obtained from reports by national and international organs addressing personal data processing and information security. Both primary and secondary resources were obtained via online desk and library research, and are all (fortunately) available in English and/or French language.

**Summary of the thesis articles/chapters**

As indicated above, this thesis is presented as a collection of publications focused on personal data security in Europe and Africa, and the effects of the EU impact on substantive African data protection law. The publications each address a specific part of the research problem under these topics, and are presented in the form of chapters. This subsection presents a brief summary of the main points of discussion each of the five publications in the thesis, and how they seek to address the problem statements highlighted above.

Chapter 1 presents an analysis of personal data security law in the EU, specifically an attempted critique of the definition of a personal data breach as it relates to a breach of security and the notification of breaches to data subjects. Contemporary EU data protection law provides for the notification of 'personal data breaches', which it summarily defines as a breach of security leading to a data compromise, indicating that an incident cannot be considered a 'personal data breach' unless it is established that it has led to a compromise of personal data. This basically means only determined data compromises can be subject to notification requirements. While this is in line with the EU risk-based approach of data protection, it tends to however exclude notification of security incidents, which by their nature and data involved, present significant risks to data subjects but following which a data compromise cannot be readily ascertained by the data controller. It is on this premise that the Chapter, after providing some clarification between a personal data breach and a breach of security in EU data

[51] Khadijah Mohamed. "Combining methods in legal research." The Social Sciences 11, no. 21 (2016): 5191-5198. 5195

protection law, suggests an alternative approach to breach notification to address this problem. It suggests that the EU legislator could either by including a risk or probability of data compromise in the definition of a personal data breach, or provide for the direct notification of data subjects in the event of a sensitive breach of security for which a resulting data compromise, for technical reasons or due to the nature of the breach itself, cannot be readily determined by the data controller or processor.

Chapter 2 discusses the state of the art of multilateral personal data security legislation in Africa, in an attempt to examine its response to contemporary data security challenges of African citizens. Following the continent's advancements in information and communication technologies, internet penetration and mobile telephony, its international community felt the need to address the data protection and security risks which these developments equally exposed the African populations to. Studies show that these developments have led Africans to produce and share massive amounts of personal data, which can be vulnerable to unauthorised access and misuse. In response to these data protection concerns, the ECOWAS and AU have both adopted corresponding legislations: the ECOWAS Data Protection Act 2010 and the AU Convention on Cybersecurity and Data Protection. The ECOWAS legislation acts as a directive for West African states, while the AU legislation will serve the same purpose for all AU member states once it comes into force.

Focusing on the personal data security (as a section of personal data protection), the article first discusses general contextual challenges which could hinder the promotion of personal data security in Africa, before examining safeguards set up by these international legislations to ensure the security of personal data of African residents. By discussing these safeguards in relation to what obtains in other jurisdictions like the EU, the article intends to demonstrate that both the ECOWAS and AU legislations come up short in some significant areas of personal data security. It should be clarified here that while there currently exist comprehensive national legislative responses to personal data security concerns among 26 African states, the article focuses solely on the multilateral response. The reason for this is to get the widest general appraisal of the current legislative landscape of personal data security in the African continent, and especially considering that many African states still do not have data protection laws, and will so far depend on these legislations to address data protection issues they may face within their respective national territories.

Chapter 3 explores the general theme of the influence of European law on African (data protection law), focusing on the impact which the EU's interpretation of examination results as personal data could have within an African educational context. Specifically, it discusses the potential benefits of according a personal data status on examination results in Africa (as is the case in the EU)

as well as some limitations in enforcing some data protection rights on these results within an African context. The article first discusses the notion of personal data as it has been defined in EU data protection texts (the 1995 Data Protection Directive and the GDPR) and which, following the reasoning of the Attorney General of the European Court of Justice, would most likely include examination results. With the EU definition of personal data being copied into African ECOWAS and AU data protection legislations, coupled with African inheritance of European law and current dependence on European case law to address grey areas in national law, the article argues that the exam results could equally be considered personal data on African soil. Based on this premise, the article then discusses the advantages which such protection could offer to African examination candidates, as well as the limitations likely to be encountered in enforcing data protection rights on examination results in the continent.

Chapter 4, in the same line as the previous article on examination results, discusses the potential impact of the EU-African data protection relationship in the education sector, focusing on the right of access to examination scripts as personal data in institutions of higher learning in Cameroon. The article makes the premise that with no national substantive data protection law yet in effect in Cameroon, the country would most probably inspire its data protection regime from the AU Data Protection Convention, either when it comes into force or if the country enacts a corresponding national legislation before then. And based on the definition of personal data in this convention, inspired by EU substantive and case law (from the *Nowak* case), and in the absence of an express provision to the contrary, examiners' evaluations on examination scripts would equally be considered personal data in Cameroon. From this premise, the article discusses the eventuality of such a development serving as a working instrument against teacher-student abuses in institutions of higher learning in the country.

Specifically, the article argues that a data protection right of a right of access to personal data, if granted to and exercised by higher education students in the country, could permit them to consult their examination scripts; and be able to verify how it was evaluated and raise objections where necessary. Such a right not yet expressly granted in national texts on student rights and obligations, and abusive lecturers who usually take advantage of this to demand sexual and other favours in exchange for grades. The article hence discusses how the right of access could contribute to forcing fair evaluation by abusive lecturers and hence limit student-teacher abuses in institutions of higher learning in the country.

Chapter 5 presents a comparative analysis between EU data protection law and African national data protection instruments, specifically the GDPR on the one hand and the Ghanaian and Kenyan data protection laws on the other hand. In essence, the article discusses the adaptation of the 1980 OECD personal data processing Guidelines into the GDPR, the 2012 Ghanaian Data Protection Act and the 2019 Kenyan Data Protection Act. The first global instrument to lay down principles of personal data processing, the OECD Guidelines set basic principles of personal data processing which have been adapted into and influenced contemporary data protection regimes worldwide. In this light, the article comparatively examines how these OECD principles have been adapted into the GDPR, the Ghanaian Data Protection Act and the Kenyan Data Protection Act.

The aim of this comparison is two-fold: in the first place, with data protection law being older and more advanced in Europe than it is in Africa, and the GDPR being one of the most significant changes in data protection regulation of the 21st Century, measuring it against the Ghanaian and Kenyan data protection acts would be a rational method of assessing the substantive quality of the African legislations. Secondly, with the GDPR adopted between the Ghanaian and Kenyan legislations, this comparison also enables the assessment of the influence of substantive EU data protection law on corresponding African national laws. The article, in this way, tries to explore the difference between pre-GDPR (Ghanaian Act 2012) and post-GDPR (Kenyan Act 2019) African national data protection laws, hence illustrate the GDPR's overseas or "Brussels effect" in Africa.

It is in this light that this paper attempts a comparative review on how these principles are consolidated in Europe and Africa: that is, between the EU's GDPR on the one hand and the Ghana and Kenyan data protection instruments on the other hand. 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 Act appears to duplicate the GDPR risk-based approach in consolidating the OECD data protection principles, the Ghanaian Act rather adopts a less rigorous approach with lesser burdens on data controllers.

**References for Introduction**


Abdulrauf, A.L., & Fombad, C.M. "The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?" *Journal of Media Law* 8, no. 1 (2016): 67-97.

Blount, M.S. *A phenomenological analysis of artistic creativity—contemporary artists' practice and philosophy*. Stephen F. Austin State University, 2007.

Bradford, A. "The Brussels Effect'. *Northwestern University Law Review* 107 (2012): 1

Bygrave, L.A. "Privacy and data protection in an international perspective." *Scandinavian studies in law* 56, no. 8 (2010): 165-200.

De Cruz, P. *Comparative Law in a Changing World*. 3rd edition. Routledge Cavendish. (2007)

De Hert, P. & Gutwirth, S. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." (2009)

De Hert, P. & Schreuders, E. "The relevance of Convention 108." Published in: *European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future*. 2001.

Fouché, C. & De Vos, A.S. "Formal formulations." *Research at grass roots: For the social sciences and human service professions 4* (2011): 89-100

Greenleaf, G. & Georges, M. "The African Union's Data Privacy Convention: A Major Step toward Global Consistency?" *131 Privacy Laws & Business International Report, 18-21* (2014).

Hornung, G. & Schnabel, C. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25, no. 1 (2009): 84-88.

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* (2013): 1-12.

Joireman, S. F. "Inherited legal systems and effective rule of law: Africa and the colonial legacy." *The Journal of Modern African Studies* 39, no. 4 (2001): 571-596

Kotz, H. & Zweigert, K. "Introduction to Comparative law." *Vol. II (T. Weir trans. 2ed 1987)* (1998).

Lee, A. & Schultz, K. A. "Comparing British and French colonial legacies: A discontinuity analysis of Cameroon." In *APSA 2011 Annual Meeting Paper*. 2011

Lynskey, O. *The foundations of EU data protection law*. Oxford University Press, 2015.

Makulilo, A. B. *African data privacy laws*. Springer International Publishing, 2016

Makulilo, A.B. "Privacy and data protection in Africa: a state of the art." *International Data Privacy Law* 2, no. 3 (2012): 163-178.

Mohamed, K. "Combining methods in legal research." *The Social Sciences 11*, no. 21 (2016): 5191-5198. 5195

O'Neill, M. "The Legal Reach of Police and Judicial Co-operation in Criminal Matters (PJCCM) Measures across EU Borders: Extraterritoriality, Territorial Extension and the "Brussels Effect". In *EU Borders and Shifting Internal Security*, pp. 139-156. Springer, Cham, 2016.

Orji, U.J. "Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act." *International Data Privacy Law* 7, no. 3 (2017): 179-189

Orji, U.J. "A Comparative Review of the ECOWAS Data Protection Act." *Computer Law Review International* 17, no. 4 (2016): 108-118

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*, pp. 105-118. IEEE, 2015.

Orucu, E., 'Developing Comparative Law' in Esin Orucu and David Nelken (eds), *Comparative Law; A Handbook.* Hart Publishing (2007) 43, 44

Reitz, J. "How to Do Comparative Law" *46 (4) AJCL (1998)*

Rich, C. "Privacy laws in Africa and the Middle East." *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA* (2014).

Rouvroy, A & Poullet, Y. "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy." In *Reinventing data protection?*,pp. 45-76. Springer, Dordrecht, 2009.

Scott, J. "Extraterritoriality and territorial extension in EU law." *The American Journal of Comparative Law* 62, no. 1 (2014): 87-126

Solove D. "Conceptualizing privacy." *Calif. L. Rev.* 90 (2002): 1096

Van der Sloot, B. "Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR." In *Group Privacy*, pp. 197-224. Springer, Cham, 2017.

Van der Sloot, B. *Privacy as virtue*. Intersentia, 2017.

Van der Sloot, B. "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?" In *Data protection and privacy: (in) visibilities and infrastructures*, pp. 3-30. Springer, Cham, 2017.

Westin, A. *Privacy and Freedom*. (Originally published in 1967). Ig Publishing. 2015 (e-book).

Wheatley, S., Maillart, T., & Sornette, D. "The extreme risk of personal data breaches and the erosion of privacy." *The European Physical Journal B* 89, no. 1 (2016): 1-12.

Wong, R. *Data security breaches and privacy in Europe*. Springer, 2013

**Chapter 1: Breach of security vs personal data breach: effect of the EU definition of a personal data breach on breach notification to data subjects**

*Currently under review at the Computer Security and Law Review journal*

**Abstract**

Contemporary EU data protection law provides for the notification of personal data breaches to data subjects if they present a high risk of harm. Personal data breaches are identically defined across EU data protection instruments as breaches of security leading to a compromise of personal data. This definition implies that for an incident to be legally considered a personal data breach and hence qualified for notification, it must involve an actual, determined or ascertained adverse effect on personal data. However, EU legislators appear to place less focus on the eventuality of security breaches which by their very nature present risks to data subjects, but are accompanied by an impossibility or difficulty to promptly determine whether or not personal data has been affected.

Against this backdrop, this article attempts a critique of the definition of a personal data breach in EU data protection law, and argues that some breaches of security by their nature could be risky to data subjects, regardless of whether a resulting data compromise can be ascertained. In the absence of the definition in EU data protection instruments, the article first discusses situations which would be considered a breach of security in EU law, inspired by information security literature and the EU NIS Directive. It then identifies the problem of limiting notification only to ascertained personal data compromises, which could be detrimental to data subjects who may be at risk of harm by the very nature of a breach of security in the absence of a determined compromise of personal data. The article then examines an alternative approach to address this limitation, which involves the substantive inclusion of a risk or probability (alongside the establishment) of a personal data compromise within the definition of a personal data breach, or alternatively, a requirement to directly notify data subjects of apparently risky breaches of security for which a resulting data compromise cannot be readily ascertained

Keywords: Breach of security, data compromise, data protection, GDPR, breach notification, personal data breach

## 1.1 Introduction

In the European Union (EU), data controllers and processors are required to implement appropriate technical and organisational measures appropriate to the risk of processing personal data, and notify data protection authorities and data subjects of personal data breaches which present a high risk to their rights and freedoms. Notifying data subjects of personal data breaches presents a significant method of protecting them against harm which could result from a compromise of their personal data, as they will be able to be on the alert against identity theft, social engineering scams or take other mitigating measures. However, based on its definition of a personal data breach, EU law allows for the notification and even recording only of incidents which have caused an actual adverse effect on personal data. In essence, it insists on two components to make up a personal data breach and hence an incident worth notifying or recording: a "breach of security" (1) which causes a compromise of personal data (2). As such, considering that not all breaches of data security are personal data breaches as has been indicated by the EU Article 29 Working Party[52], complying to the breach notification requirement necessitates an understanding by data controllers and processors of what exactly constitutes a personal data breach and a breach of security in EU law, as well as their ability to separate both concepts. However, EU law so far has not concisely clarified the conceptual difference between a breach of security and a personal data breach, though it is clear from the law's definition of the latter that both concepts are very much related. And more importantly, by focusing on the notification only of incidents which can be ascertained or determined to have led to a compromise of personal data, the law appears to overlook the possibility of harm to data subjects caused by data compromises which may be technically difficult or practically impossible to ascertain following a breach of security.

Personal data protection law in Europe has considerably addressed (personal or non-personal) data breaches, spread across at least eleven instruments[53]. Among these are four laws regulating personal data protection, namely the General Data Protection Regulation[54] (GDPR), the Data Protection Regulation for EU Institutions[55], the Data Protection Law Enforcement Directive (popularly referred to as the Police Directive)[56] and the Directive for the processing of personal data over public electronic

[52] See infra

[53] Maria Grazia Porcedda, 'Patching the patchwork: appraising the EU regulatory framework on cyber security breaches' (2018) Computer Law & Security Review 34, no. 5, 1077-1098, 1079

[54] 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)

[55] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

[56] 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,

networks (known as the ePrivacy Directive)[57]. They all adopt an identical definition of a personal data breach, 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*'[58]. They equally require, as mentioned above, that these personal data breaches be recorded and, in the event of high risk to data subjects, notified to the latter.[59] However, they do not define a "breach of security", an oversight common among other EU instruments addressing information security.[60] Even the Article 29 Working Party[61] (WP29) appears to have overlooked the concept so far. In its Opinions addressing personal data breaches[62], the data protection advisory body expounded on the parts of above definition of a personal data breach relating to a compromise of personal data (destruction, loss and loss of access to, alteration and unauthorised disclosure of or access) without elucidating on the "breach of security" component. It does insist, however, that only "personal data breaches" (breaches of security which are determined to have actually led to an actual adverse effect on personal data) are subject to breach notification requirements.

It is in this context that this article argues that while making actual data compromise a condition for notification admittedly helps focus protection only on data subjects with a real risk of harm, it however tends to overlook the eventuality of a breach of security whose effect on personal data may not be easily or promptly determined by the data controller considering the nature and circumstances of the incident, or even with state of the art technology in place. It seeks to first of all provide an understanding of what would constitute a breach of security in EU data protection law, before making a case that they could by their very nature present real risks to data subjects in the absence of a determined compromise of personal data. The lack of a certain compromise of personal data would

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

[57] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[58] Article 4(12) GDPR, Article 3(11) of Regulation 2016/680, Article 2(h) of Directive 2001/136/EC (amending Directive 2002/58/EC), Article 3(16) of Regulation (EU) 2018/1725

[59] See Articles 33 and 34 GDPR, Articles 34 and 35 of Regulation (EU) 2018/1725, Article 4(3) of the ePrivacy Directive (Consolidated version including amendments), Articles 30 and 31 of Directive (EU) 2016/680.

[60]Porcedda notes a general lack of a definition a 'breach' in EU instruments bearing on (non-personal) data security like the Directive 2009/140/EC (The Better Regulation Directive), Regulation 910/2014/EU (Electronic Identification and Assurance Services (eIDAS) Regulation), Directive 2015/2366/EU (Payment Services Directive) and even Directive 209/1148/EU (the Network and Information Security (NIS) Directive). See Porcedda, (n.10). p.1081

[61]The Article 29 Working Party was created by Article 29 of the Data Protection Directive as the EU advisory authority on the matters of data protection. It was replaced by the Data Protection Board under the GDPR.

[62] The Article 29 Working Party. 'Guidelines on Personal data breach notification under Regulation 2016/679 (WP250)' and 'Opinion 03/2014 on Personal Data Breach Notification (WP213)'

consequently prevent notification to data subjects under the current approach, and hence limit protection for data subjects in such cases. The article then suggests and examines the inclusion of a probability or risk, alongside the establishment of data compromise into the current definition of a personal data breach as an alternative approach to address this limitation.

### 1.2 'Breach of security': a brief information processing overview

There is some considerable literature bearing on what constitutes a breach of security in terms of information processing and management. To begin with, Black's law dictionary defines a 'breach' as 'a violation or infraction of a law or obligation.'[63]This is a common definition in law, especially tort law, where a breach of contract means [negligent or intentional] non-respect of or failure to perform one's duties as specified by the terms of a contract.[64] In terms of an employment relationship for example, a breach could refer to the cognitive evaluation that an organisation is failing to fulfill its obligations to the employee[65], and/or vice versa. In a nutshell, a breach is generally interpreted to mean non-respect of or failure to follow pre-determined rules or principles of a specific domain of activity.

It follows from the above that a breach of security would refer generally to the non-respect of or failure to comply with pre-determined security principles and rules. This approach is not so different from a general use of the term in relation to information security; where it would include (but may not be limited to) a failure to comply or ensure compliance with information security principles. Michael Krausz, in his 2015 book titled *Managing Information Security Breaches*, proposes a definition of the term 'breach' in light of the confidentiality, integrity and availability of information flows within an organisation. He contends that a breach of confidentiality 'occurs every time the need-to know principle, on which all dissemination of information should be based, is *violated*' (emphasis added), noting that the breach does not occur when damage becomes visible, but occurs at the point in time when the company's security guidelines have been violated.[66] A breach of availability 'can occur when the availability of your IT systems is *reduced* due to an adverse event…e.g. a virus…or when the Service Level Agreements (SLAs) that are in place are *not adhered to*, quite independently of any actual damage that may, or may not, result'(emphasis added).[67] And an integrity breach occurs 'whenever the integrity of information or its means of storage are *violated*, for example, by

[63] Bryan A. Garner (ed). "Black's Law Dictionary—Ninth Edition.' *Thomas Reuters.* (2009).
[64] See Rita S. Kohn. "The Model Contract." *Ent. & Sports Law.* 11 (1993): 9.11
[65]Guo-hua Huang, Xiongying Niu, Cynthia Lee, and Susan J. Ashford. 'Differentiating cognitive and affective job insecurity: Antecedents and outcomes.' *Journal of Organizational Behavior* 33, no. 6 (2012): 752-769.753
[66] Michael Krausz. *Managing information security breaches: studies from real life*. IT Governance Publishing, 2015.52
[67] Ibid, 53

transmission errors, by intentional manipulation, by unintentional handling errors or by the corruption of file content or structure due to electrical, magnetic or other failures' (emphasis added).[68]

It is worthy to mention here that the concept of a breach of security in the physical realm is not so different from that of an information management context. In both instances, there is the prevailing idea of an overarching security infrastructure composed of technical measures and procedural rules which are respectively bypassed or not complied with. For example, Skinner defines a breach of security as 'a successful attack on a computer system's security controls in order to penetrate the system to acquire or corrupt information on the system, thus disrupting the confidentiality, integrity, or availability of the information on the system', noting that these attacks can come from outside or from within a company or institution.[69] Manro et al further contend that physical breaches of security also consist a threat to information security, advancing that they refer to situations where 'somebody with malicious intent has physical access to the hardware where either your application is running or where your data is stored.'[70] They equally note however that in the domain of information security, physical security consists (or should consist) of first layer security, and if other forms of security which protect the hardware are in place [e.g protective metal cages], a physical security breach may not always result in loss of data.[71] An illustrative example will be an intruder who, with the intention of physically destroying a server storing data, breaks into a data centre by forcing open the main door (hence bypassing first layer security), but discovers the targeted server is protected in a reinforced steel cage, which he cannot open or break. So though there was a physical security breach, there was no effect on processed data.

While Skinner and Manro et al focus on the physical threats to a system, Krausz on the other hand, as suggested by the terms 'violated', and 'not adhered to', perceives a breach of security as a situation in which standard rules of information management within a given institution or information management protocol are not respected, and which could be purely of technical as well as human origin. However, they both importantly concur on a crucial element: the occurrence of a breach of security does not depend on actual damage caused to processed information: a breach occurs once a security rule or protocol is not complied with or in the event of a physical threat to a security infrastructure. It therefore could flow from this interpretation that a breach of security would mean

[68] Ibid, 54
[69] Timothy H. Skinner. 'California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet A Suitable Template For National Identity Theft Legislation.' *Rich. JL & Tech.* 10 (2003):2.
[70]Rajan Manro, Rajneesh Randhawa, and A. Joshi. 'Security Issues in Cloud based e-Governance model.' *International Journal of Computers & Distributed Systems* 1, no. 1 (2012): 14-16.14
[71] Ibid

either of two aspects: the sheer non-respect of security rules and protocols (of a given information management process within an organisation) or the breakdown or bypass of a physical or technical security infrastructure. And both regardless of whether processed information was actually compromised. Both positions are apparently adopted into the rules of secure processing in EU data protection law.

### 1.3 'Breach of security' in the EU data protection law

As mentioned above, EU data protection laws do not define the term 'breach of security'. However, they all contain provisions addressing secure rules of processing personal data, which could serve as a starting point to arrive at an interpretation of what would legally consist a breach of security. For example, Article 32 of the GDPR, titled 'Security of Processing', states as follows:

'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing… the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'[72]

This provision appears to incorporate both approaches of a breach of security discussed above in Section 2: as a violation of determined security rules and as the occurrence of an actual adverse effect on processed personal information. The following subsections explain this further.

#### 1.3.1 Breach of security as non-compliance to EU data protection rules of secure processing

As regards non-compliance with rules of secure processing, the above Article 32(1) requires data controllers and processors to implement, among others, "organisational measures" to ensure secure processing. These organisational measures refer to rules within the controller's premises which should be followed to avoid incidents or situations which could be detrimental to secure processing, and

[72] Also see Article 33 of Regulation (EU) 2018/1725, Article 29 of Directive (EU) 2016/680

therefore regard the human factor of secure processing. As Wood observes, information security used to be a strictly technical issue, but as the use of computer networks evolved, measures to ensure their security also had to evolve and extend beyond the technical to include other organisational measures, like human input.[73] It is also well documented that besides security software and hardware, a secure information system includes human staff with adequate security-awareness training to prevent them accidentally destroying or losing information, or falling for social engineering scams[74]. Data controllers are therefore expected to implement rules within their organisations to prevent conducts which could put the security of processed personal data at risk e.g. prohibiting employees from taking home laptops which contain sensitive personal data, confirming the integrity of employees through lawful background checks, training staff on confidentiality etc. The same rule applies for technical measures: controllers and processors are expected to use software, hardware or other available techniques to secure and ensure unperturbed processing as stated in subsections (a) to (d). In line with Krausz's observations, non-compliance with these measures (either by their non-respect by staff or their non-implementation by the controller or processor) within an organisation will constitute a breach of security.

It is worth mentioning here that in contemporary data protection law, security measures are essentially contextual and could be tricky to determine, with companies sometimes left with little or no guidance as to what types of security measures they should take in a given processing situation to be compliant.[75] This is similar in the EU, where the requirement for data controllers to take 'technical and organisational measures…appropriate to the risk' only spells out a rather vague standard of security to adhere to, hence could make uncertain the exact rules of security to comply with. However, the phrase 'Taking into account the state of the art, the costs of implementation… scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons…' sets the guidelines controllers should take to guarantee secure processing. The issue here, though, is that the burden lies on the controller and processor to translate the standard into context and determine what security measures to take. In other words, the controller is expected to use these provisions as a strict guide to determine the level or type of security applicable to a processing

[73] Charles Wood, 'Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature' (2004) Computer Fraud & Security 2004, no.1: 16-17

[74] Michael E. Whitman & Herbert J. Mattord, *Principles of Information Security* (Cengage Learning, 6th edn, 2018) pp 21-23

[75] See John Beardwood and Mark Bowman. 'Cybersecurity Evolves. Understanding what constitutes Reasonable and Appropriate Privacy Safeguards Post-Ashley Madison.' *Computer Law Review International* 17, no. 6 (2016): 166-172.166

procedure, and then comply with them; like some sort of guided self-regulation. It has already been observed that in contemporary EU data protection law, the main responsibility to determine how to apply data protection principles is left to the controllers and processors. The Data Protection Authority (DPA) acts more like a subsidiary regulator; a position justified by the EU regulator's intent to 'simplify the regulatory environment' and 'substantially reduce the administrative burden on data controllers and processors'.[76]

The rules of secure processing of personal data in the EU are therefore contextual and not fixed or permanent: they emerge in correlation with the particular risk involved in a particular processing situation. Discussing the GDPR, Gellert argues that the law could essentially be portrayed as a risk management legislation,[77] with risk being 'the chance (understood as a probabilistic notion) that a danger (i.e., an event with harmful consequences) will happen.[78] The controller and processor are required take measures 'appropriate to the risk [of processing]'i.e. take measures (depending on the cost, purpose, state of the art technology and nature of data collected) which ensure that the data subject is protected from any probable danger which could arise from a specific processing activity. So whether or not a rule of security exists in the first place depends on whether or not there exists any risks with regard to processing a specific type or category of data; a method of regulation referred to as the risk-based approach[79]. It is worth noting though that the WP29 has stressed that the risk-based approach should not be interpreted to mean no security measures should be taken where there is little or no processing risk[80].

### 1.3.2 'Breach of security' as an actual defeat of a security infrastructure in EU data protection law

Considering the technical nature of this section, the discussion shall be based on the provisions of EU law on information security, specifically Directive (EU) 2016/1148[81], known as the Network and

[76] Maria Eduarda Gonçalves. 'The risk-based approach under the new EU data protection regulation: a critical perspective.' *Journal of Risk Research* (2019): 1-14.3-4

[77] Raphaël Gellert, 'Understanding data protection as risk regulation.' *J. Int. Law* 18, no. 11 (2015): 3-16.

[78] Ibid, p.8

[79] For a discussion on the risk-based approach in EU data protection law, see Maria Eduarda Gonçalves. 'The risk-based approach under the new EU data protection regulation: a critical perspective.' (supra).

[80] It is worth noting though that the Article 29 Working Party has stressed that the risk-based approach should not be interpreted to mean no security measures should be taken where there is little or no processing risk (The Article 29 Working Party. 'Statement on the role of a risk-based approach in data protection legal frameworks'. (WP218). 30th May 2014). The advisory body maintains that security measures must be equally strong when processing is relatively 'low risk'. Accordingly, the risk-based approach should just be considered as demanding additional measures when risks are identified, not evading strict security compliance in some situations (See Maria Eduarda Gonçalves. (2019) ibid). Yet, it admitted that a data controller whose processing is relatively low-risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk.

[81] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

Information Security (NIS) Directive. This can be justified on grounds of the close interplay between EU data protection law and the NIS Directive. First, that Recital 49 of the GDPR adopts an almost identical word-for-word definition of 'network and information security' as defined in Article 4(2) of the NIS Directive. Also, Article 15(4) of the NIS Directive requires the Directive's Competent Authority to 'work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.' This is evidence that both instruments run parallel to (and hence could be expected to complement) each other in their respective network security and data processing regulation activities.

The NIS Directive defines network and information security as 'the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems[82]', and an 'incident 'as 'any event having an actual adverse effect on the security of network and information systems'[83]. A network or system's security therefore, according to the NIS Directive, is its ability to resist an adverse effect on data processed within. No further guidance is given on the interpretation of an 'actual adverse effect' which could broadly be interpreted to range from minor events with insignificant consequences to serious and highly costly network damage. Because nothing in the Directive suggests this adverse effect must be serious enough to compromise data processed within a network or system, and with 'security' meaning 'ability to resist', an event could still therefore qualify as a security incident (and hence breach of security) if it as much as slightly and temporarily disrupts the ability of a system to resist an action which could compromise processed data. Or if the event temporarily but insignificantly disrupts the availability of a service provided over a network.

Based on the above, and the documented relationship between the NIS Directive and EU data protection law, the slight or complete disruption of a system's ability to resist an action which could compromise processed data would constitute a breach of security in EU data protection law. This is also in line with the observations by Skinner and Manro et al in Section 2 that a breach of security manifests in an actual defeat or weakening of the security infrastructure.

The last two Sections jointly map out the scope of a breach of security in EU data protection law. From this analysis, and viewed with the definition of a personal data breach across EU data protection

[82] Article 4(2) NIS Directive
[83] Article 4(7) NIS Directive

instruments, the principal difference between both concepts is much clearer: for an incident to qualify as a personal data breach in EU data protection law, it must have led to the compromise of personal data. While the objective of this requirement could understandably be to prevent over-reporting of personal data breaches to data protection authorities, it nevertheless may limit protection available to data subjects in the event of a breach of security which, without legally attaining the status of a personal data breach, poses significant risk to data subjects.

### 1.4 Breach of security vs Personal data breach in the EU data breach notification: the problem

One of the innovations of EU data protection reforms of the early 2010s was the introduction of the personal data breach notification requirement for data controllers and processors, requiring that they inform data protection authorities and data subjects of personal data breaches which are "likely to result in a high risk to the rights and freedoms" of data subjects.[84] In its Impact Assessment accompanying the proposed GDPR, the EU Commission identified three advantages of notification: they provide a systematic feedback about the actual risk and the actual weaknesses of existing security measures; enable authorities and consumers to assess the relative capabilities of data controllers with respect to data security; and force data controllers to assess and understand their own situation regarding security measures."[85] In essence, data subjects are required to be informed of personal data breaches which present high risks to their rights and freedoms (e.g. if the breach involved sensitive health or financial information) so they can take necessary measures to prevent further harms, like identity theft or falling for social engineering scams. While this requirement contributes to safeguarding online security and trust between data subjects and those handling their data, it features a setback which could impede on the high-level protection of data subjects: the law requires the notification and reporting of 'personal data breaches', and not 'breaches of security'.

There have always conceptual overlaps in information security literature between the terms 'data breach' and 'security breach'[86], as well as with terms like 'data leakage'[87] or 'data spill'[88], all being

[84] Article 34 GDPR, Article 35 Regulation (EU) 2018/1725, Article 31 Directive (EU) 2016/680

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

[86] Sasha Romanosky, David Hoffman, and Alessandro Acquisti, 'Empirical analysis of data breach litigation' (2014) Journal of Empirical Legal Studies. 74-104, 79; Sasha Romanosky, Rahul Telang, Alessandro Acquisti, 'Do data breach disclosure laws reduce identity theft?'(supra)

[87]Shahidul Islam Khan, Abu Sayed Hoque, 'Development of national health data warehouse Bangladesh: Privacy issues and a practical solution' (21 December 2015) 18th International Conference on Computer and Information Technology (ICCIT) 373-378, 375.

[88] R. Barona & Mary Anita. 'A survey on data breach challenges in cloud computing security: Issues and threats.' Presented at the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) 2017 Apr 20 (pp. 1-8). IEEE.

used to refer to very similar occurrences. However, as discussed in the introduction, the EU legislator opted for a definition of a personal data breach as a breach of security which has caused or at least is ascertained to have caused a compromise of personal data. In other words, it involves the non-compliance of a technical or organisational security measure of data processing or an actual defeat of a security infrastructure (X) accompanied by an adverse effect on personal data (Y). This implies that the presence of (X) and absence of (Y) legally disqualifies an incident as a personal data breach, hence that incident may not be reported in contemporary EU law. This is reiterated by the WP29 Guidelines on Personal Data Breach notification under the GDPR and European Data Supervisor (EDPS) Guidelines on personal data breach notification for the European Union Institutions and Bodies. Both Guidelines maintain that not all breaches of security are personal data breaches[89], and emphasize on the establishment of a compromise to personal data (Y) for a breach of security to become a data breach in order to fall within the breach notification requirement[90]. However, this may be problematic in the event where an incident (X) may present a real risk for data subjects, yet a corresponding compromise (Y) cannot be determined or ascertained in a timely manner, even with state of the art processing infrastructure in place. An example is the Whatsapp Ireland security breach of May 2019.

On 13th May 2019, in a statement released by the Irish Data Protection Commissioner (DPC)[91], Whatsapp Ireland informed the Irish DPC of the discovery of a security vulnerability on their platform, presupposing the installation of malware by a malicious attacker which could have led to the harvesting of personal data of WhatsApp users. However, WhatsApp Ireland could not officially notify the incident to the competent European data protection authorities under Article 33 of the GDPR because at that point they were "still investigating as to whether any WhatsApp EU user data has been affected as a result of this incident." It should be pointed out that Article 33 is titled "Notification of a *personal data breach* to the supervisory authority" and not "Notification of a *security incident*…", hence Whatsapp Ireland's apparently compliant restraint from notifying EU data protection authorities To this can also be added Regulation No 611/2013 which states that a 'detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that

[89] European Data Protection Supervisor *Guidelines on personal data breach notification for the European Union Institutions and Bodies*. Adopted 21st November 2018. Paragraph 26.; Article 29 Working Party *Guidelines on Personal data breach notification under Regulation 2016/679* (supra) p.7

[90] European Data Protection Supervisor *Guidelines on personal data breach notification for the European Union Institutions and Bodies* (ibid) Paragraph 25, Article 29 Working Party *Guidelines on Personal data breach notification under Regulation 2016/679* (ibid) p.11

[91] Data Protection Commission Statement – Whatsapp Security Incident (14th May 2019), retrieved from https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-whatsapp-security-incident Accessed 20th May 2019.

a security incident has occurred that led to personal data being compromised…'[92], further indicating that a data breach is a two-factor event: security incident + determined compromise of data. Also, Whatsapp Ireland in this situation are not required by law to even record or document the incident under Article 33(5) GDPR, because the provision requires documentation of personal data breaches. Though Whatsapp Ireland nevertheless urged its EU users to update the application as a post-breach security measure as later indicated in the statement, this situation illustrates an important limitation in the definition of a personal data breach in EU data protection law.

As discussed above, the WP29 reiterates the inseparability of a breach of security and compromise of data in its analysis of when a data controller should be considered as being aware of a personal data breach. The advisory body noted that a controller shall be deemed "aware" when that controller "has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."[93] While admitting that with some incidents it may take some time to establish whether a breach of security has led to a data breach, it goes further to state that the GDPR nevertheless requires data controllers to take prompt technical and organisational to immediately investigate and establish if a breach has occurred. However, it notes that during these investigations, the data controller shall not be considered "aware" of the breach.[94] Worth noting in this analysis is the WP29 apparently focusing the awareness test on the "data breach" with not much focus on the "breach of security". In other words, there is no responsibility on the controller towards the data subjects when the controller becomes "aware" of a breach of security. Such responsibility is triggered only when it finally establishes a resulting compromise of personal data (e.g. the 72-hour deadline to notify the supervisory authority (Article 33 GDPR) begins counting from the moment a resulting compromise of personal data is ascertained, apparently not when the initial breach of security is discovered). It would therefore appear the WP29 places little consideration on the eventuality of a breach of security in which, for example, a resulting data compromise takes a long time to ascertain even with state of the art infrastructure.

In line with the risk-based approach, Article 24 GDPR requires data controllers to process data in general consideration of the likelihood and severity of risks of data subjects. Recital 76 GDPR states that such likelihood and severity of risk to the data subject should be determined by reference to the

[92] Article 2(2), Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications
[93]Article 29 Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. p.11 (supra).
[94] Ibid

nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is determined whether data processing operations involve a risk or high risk. These provisions portray the pivotal significance of risk in contemporary EU data protection law, and would customarily be the principal concern when identifying or reporting personal data breaches i.e. only data compromises which present a high risk to data subjects need to be notified to the latter. However, to comply with the notification requirement, it appears the law places importance on risks which an already determined data compromise may expose data subjects to, but not so much consideration of risks which a security incident in itself, regardless of whether or not there is a determined compromise of personal data, can cause data subjects. This appears to set aside, from the scope of data subject notification, breaches of security which by their nature present real risks of data compromise and danger to data subject rights, but without such compromise being ascertained. It is on this basis that this article seeks to discuss an alternative approach which address the above-identified limitations of personal data breach reporting as a protective measure for data subjects.

### 1.5 Breach of security vs personal data breach in EU law: an alternative approach

As discussed above, EU data protection law places extreme importance on risk; the term "risk" even being mentioned up to 75 times in the GDPR. Organisations processing personal data have to build and implement compliance programs based on the "likelihood and severity" of risks and potential harms to the individuals. And as discussed in Section 2, the ability of data controllers and processors to anticipate and prevent or reduce risks to data subjects forms the basis of secure processing, as well as other notions like data protection by default or by design. In order to further consolidate the risk-based approach in protecting individuals and fortify online trust, this article opines that a conditional risk of compromise factor could be incorporated in the normative definition of a personal data breach. Or otherwise, data subject notification can be extended from classic and risky personal data breaches to include breaches of security which by their nature present a real risk of data compromise. It should however be noted that both approaches are inextricably related, and the implementation of one may tend to render the other obsolete or unnecessary. Nevertheless, their separate examination appears necessary to better appreciate their respective impacts on the protection of data subjects. Also, in light of the constant evolution of information security, both approaches may need to co-exist and complement each other to solve future legal problems in the domain of personal data security.

#### 1.5.1 Including a 'risk of data compromise' factor in the definition of a personal data breach

As examined above, the inseparability of a breach of security on the one hand and a resulting, determined compromise of processed personal data on the other hand within the definition of a

personal data breach in EU data protection law creates a sort of grey area as regards to regulating a breach of security in relation to data subject notification. Certainly, it can always be argued that failure to implement technical or organisational measures to ensure a level of security appropriate to the risk of processing would be a *prima facie* infringement of EU data protection rules and would likely fall under the investigating and sanctioning competence of a supervisory authority. However, the law is silent as to whether these infringements can also be notified to data subjects if they in themselves present a likelihood of risk to their rights and freedoms in the absence of an ascertained compromise of personal data. For example, where the security attack was so sophisticated even state of the art technology cannot ascertain the extent of the a compromise in a timely manner. And this mainly because contemporary EU data protection law does not provide for the notification to data subjects of "breaches of security", but rather of "personal data breaches".

A solution to this could be to modify the definition of a personal data breach to include a risk, alongside the establishment, of a compromise to personal data. That is, an incident may be legally qualified as a personal data breach if there is reason to believe that it presents a risk or probability of a compromise to personal data. A personal data breach may therefore be defined as "a breach of security leading to *or presenting a (high) risk of* an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The essence of this definition in relation to data subject notification is that a prior risk factor is now placed between the breach of security and the compromise to personal data, and not just between the compromise and any eventual impact on data subjects. So once a breach of security is noticed, its eligibility for data subject notification may be considered at two levels: first, what are the odds, by its very nature, that it indeed can lead to a data compromise? And secondly, how harmful can this compromise be to data subjects?

It is worth mentioning here that the inclusion of a (high) probability of data compromise in the technical definition of a data breach has been considered in information security literature. Krausz for example observes that a "breach" in information security means damage to confidentiality, availability or integrity of information has actually occurred, *or is bound to occur*, if mitigation of a risk does not set in immediately [95](emphasis mine). By incorporating the consideration of a (high) risk or probability of a data compromise in the substantive definition of a data breach (as opposed to its certainty or establishment in EU data protection law), this approach finds worthy of attention incidents which have

[95] Michael Krausz. *Managing information security breaches: studies from real life* (supra) 61.

not yet led to a data compromise. An information security incident can thus be considered a 'data breach' in the absence of a data compromise, but undoubtedly with a reasonably strong certainty that the incident would eventually lead to a data compromise.

The resulting effect of the above suggested definition would be that the breach of an organisational or technical security measure, or the breakdown or defeat of a security infrastructure would be legally considered a personal data breach once there is a probability that it may have led to the compromise of personal data. As such, once a controller processing highly sensitive data notices a breach of security, it may not need to carry out an investigation to ascertain the compromise of personal data in order to apply breach regulatory measures like notification or recording, as currently required across the EU data protection laws. All it needs is reasonable certainty that a compromise would have occurred following the incident. It should be pointed out here that while EU law, admittedly, does put an obligation on the controller and processor to gear up technically and organisationally to ensure that they are "aware" of any data compromises in a timely manner so that they can take appropriate action[96], this may not always be feasible especially in light of the increasing sophistication of cyberattacks. The result could be considerable time taken by a controller, who discovers a breach of security, to investigate and ascertain a data compromise in order to be deemed "aware" of an incident and have it qualified as a personal data breach within the meaning of EU law and suitable for any further legal actions provided for such incidents; by which time much damage may have already been done to data subjects. The focus on a risk (rather than certainty) of a data compromise thus broadens the scope of a personal data breach, and implies additional protection for data subjects.

### 1.5.2 Notification of risky breaches of security (rather than 'personal data breaches') to data subjects

As an alternative to modifying the current definition of a personal data breach by EU data protection law, another means of optimizing the risk-based approach and ensure high-level protection could be the provision for the direct notification of risky breaches of security to data subjects in the absence of an ascertained data compromise. In essence, similar to the effect of a modified definition as discussed above, this inclusion would require controllers to notify data subjects of risky security incidents without the need to first ascertain whether personal data was actually compromised. The test for notification, as opposed to the current approach, shall be the inclusion of a (high) risk or probability that personal data has compromised, in addition to the certainty or actual determination of a

[96] See Recital 87. Also Article 29 Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. (supra) p.11

compromise. It therefore could be the responsibility of controllers to take into account the context of processing, nature of a breach of security to immediately decide whether it is most certain that data was compromised. And considering the sensitive nature of the data, whether or not to notify the data subjects. It should however be noted that the implementation of encryption or other forms of protection on the compromised data, as listed in Article 34(3) GDPR for example, would mean low risk of harm of data subjects, hence there may be no need to notify data subjects.

This is illustrated in the following tables:

**Current notification regime**

| **Step 1** | **Step 2** | **Step 3** |
|---|---|---|
| Controller/processor discovers breach of security | Investigates to establish a compromise of personal data (to fulfill the definition of a data breach) | Notifies data subjects in case of a determined data breach of high risk (subject to the additional security exceptions of Article 34(3)) |

**Alternative approach**

| **Step 1** | **Step 2** | **Step 3** |
|---|---|---|
| Controller/processor discovers breach of security | Assesses whether there is a risk or probability that data may have been compromised | Notifies data subjects in the event of a risk or probability of compromise, without need of certainty (subject to the additional security exceptions of Article 34(3)) |

A significant aspect of this proposed approach is that basing the need to notify on risk rather than certainty of a data compromise tends to place the protection of data subjects as a priority over compliance with the requirement to ascertain the compromise of personal data. A controller for example who discovers a breach of security and launches an investigation to ascertain a data compromise before notifying will be in compliance with the Regulations (with regard to the definition of a data breach) which require that he investigates to ascertain a data compromise. However, this time

lapse for investigations may be detrimental to data subjects if sensitive data may already have been compromised, especially where the attack was highly sophisticated and makes it difficult to promptly confirm the data compromise.

It is worth noting however that this approach not totally new and has actually been envisaged, albeit hypothetically to say the least, by data protection experts. The UK Information Commissioner (ICO), on its website, adopts a similar reasoning in one of its fictional examples of a personal data breach notification under the GDPR which would be considered appropriate by a data controller.[97] It examines the case of an employee who loses a briefcase containing a laptop and paper files. The employee tells his manager that he believed the laptop was encrypted and the paper files were redacted. The manager reports the incident to the IT department, which remotely wipes the laptop. The data controller did not report the breach as they believed there was little or no risk to data subjects. However, the IT department later discovers the employee was working on an old laptop, which was not encrypted or password protected. The employee also confirms that the paper files were for an upcoming criminal trial and the personal data, which related to criminal convictions and health information, had not been redacted. The controller then reports the breach to the ICO and informed the data subjects. In such a case, the ICO observed that once the controller discovered the laptop and papers were not secured, they made the right decision to notify the individuals concerned and the ICO, because there was a period of time within which somebody could have accessed sensitive data. There was no way for the controller to know what had happened to the data, so they cannot be certain that it was unlikely a risk to the data subjects would occur. Notification was therefore based on (high) risk rather than certainty of a compromise of personal data.

This approach could be significant in cases where it is almost impossible or time-consuming for a controller to know or determine a compromise of personal data in order for an incident to fall within the definition of a personal data breach, and hence satisfy the notification requirement. In the above example, the loss of the unencrypted laptop and unredacted papers and the time lapse to discover that they were unprotected presents a breach of security which could be risky to the data subjects if data actually got compromised. No compromise could be ascertained at that point, so normatively there was no personal data breach as defined by EU data protection law. However, considering the sensitive nature of the personal data and high risk to which the data subjects would be exposed if the data was compromised, it seemed only reasonable to notify the data subjects so they can take protective

[97] Information Commissioner's Office. *Personal data breach examples*. Retrieved from https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/. Accessed 6th June 2020.

measures. Thus there was no ascertained compromise of personal data (hence no 'data breach' as defined by Article 4(12), yet the ICO recommends that the data subjects nevertheless to be notified due to (high) risks of a compromise to their fundamental rights and freedoms.

Despite the apparent higher level of protection to data subjects it offers, this approach could nevertheless be exposed to some criticism. An obvious one would be that it may direct data controllers to report incidents which do not end up in the compromise of personal data or provoke just a trivial compromise with no substantive impact. This could lead to the over-reporting of incidents and unnecessary alerts to data subjects which may cause unfounded and unnecessary panic and distress.

Another issue would be the determining an appropriate level of probability of exposure of personal data to warrant notification, i.e. in what situations should a breach of security be considered to be bound to lead or cause a compromise of personal data, so data subjects may be informed? As already discussed, the risk-based approach of EU data protection law requires controllers and processors to adopt stricter security measures for processing which involve higher risks to the rights and freedoms of data subjects. This implies that breaches of security which only affect part of a security system or are too weak to have led to any compromise of personal data would not need to be reported. However, it appears determining whether or not a breach of security was in itself serious enough to have exposed personal data to certain compromise will require an investigation by the controller; which could also be time consuming or technically difficult to conclude depending on the sophistication of the attack. It is however opined here that just as the European Union Agency for Network and Information Security (ENISA) developed a methodology framework for the assessment of the risk which a compromise of personal data could present to data subjects[98], a similar framework could also be developed to estimate, in the first place, the probability and/or risk of exposure of personal data following a breach of security. Despite these criticisms however, informing data subjects of risky security breaches so they stay alert and take appropriate measures before determining if there has been a compromise of personal data could arguably be a more preventive approach to securing their rights and freedoms.

## 6 Conclusion

It would appear the risk component in personal data security enforcement in the EU is triggered on personal data breaches, rather than on breaches of security. In other words, EU data protection law currently focuses on the risks presented by an ascertained or determined compromise of personal data

[98] ENISA. *Recommendations for a methodology of the assessment of severity of personal data breaches*. Working Document, v1.0, December 2013

to data subjects, rather than on whether the initial security breach itself could be risky to data subjects where an actual compromise of personal data is uncertain. As seen with Recital 87 of the GDPR, the law only requires data controllers to adopt technical measures to be able to quickly ascertain the compromise of data, without much substantive consideration on cases where such compromise could be difficult to establish even with state of the art threat-detection measures. While the current regime helps prevent over-reporting or notification of trivial incidents, the need to determine or ascertain the compromise of personal data in a security incident may limit the protective options available for data subjects in EU data protection law.

It is on this assertion that this article set out to examine another alternative approach to personal data breach enforcement to address this limitation. It begins by determining what would constitute a breach of security under EU law data protection law. In the absence of a definition of the term in EU data protection texts, this necessitated a review of information security literature before relating the main findings to EU data protection rules on secure processing and the provisions of the NIS Directive relating to information systems and network security. This analysis concludes that a breach of security in EU data protection law would mean either non-compliance to the rules of secure processing, or an actual breakdown or defeat of a security infrastructure protecting processed data. The article then moves to discuss the relationship between a personal data breach and a breach of security in light of the personal data breach notification and recording requirements across EU data protection texts. In doing so, it highlights the law's requirement for the presence of a compromise of personal data for an incident to qualify as a personal data breach, a fact which, the article argues, could limit the protection of data subjects especially where the circumstances are such that the data compromise cannot be promptly determined. And this even with state of the art security or threat-detection measures compliantly put in place by the data controller in accordance with the data protection rules of secure processing. It is also pointed out that this observation has already been made by the ICO of the UK in one of its hypothetical personal data breach notification examples on its website.

To address this limitation, the article envisages the modification of the definition of a personal data breach in EU law to also include, in addition to the establishment of a data compromise, a (high) or risk or probability of a data compromise. As such, data controllers (and/or processors) would not be expected to investigate a breach of security to ascertain a compromise of personal data before informing data subjects; the only test being that they reasonably believe, based on the nature of the security incident, that personal data is bound to or is most likely to have been compromised, as well as the sensitive nature of the data. This approach however is not void of criticisms however, one being

the risk of over-reporting or notification of security incidents which end up not leading to or provoking an insignificant compromise of personal data to the data subjects. Another issue concerns determining a test of being reasonably certain that an incident is risky enough or would be bound to cause a data breach. In light of the risk-based approach, it may be a tricky task to determine situations in which data controllers and processors should be expected to consider that a breach of security is bound to lead to a personal data compromise, so they may notify data subjects. It is opined here that some guidance could be developed to help controllers and processors pre-determine if a security incident is reasonably bound to cause, or if there is a high probability that it will lead or has led to a compromise of personal data. Similar to the methodology framework developed by ENISA to help data controllers and processors determine the severity of an ascertained personal data breach on data subjects.

**References for Chapter 1**

Barona, R. & Anita, E.A. "A survey on data breach challenges in cloud computing security: Issues and threats." Presented at the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) 2017 Apr 20 (pp. 1-8). IEEE.

Beardwood, John and Bowman, Mark. "Cybersecurity Evolves. Understanding what constitutes Reasonable and Appropriate Privacy Safeguards Post-Ashley Madison." *Computer Law Review International* 17, no. 6 (2016): 166-172.

Garner, Bryan A. (ed). "Black's Law Dictionary—Ninth Edition." *Thomas Reuters.* (2009).

Gellert, Raphaël. "Understanding data protection as risk regulation" (2015) *J. Int. Law* 18, no. 11: 3-16.

Gonçalves, Maria E. "The risk-based approach under the new EU data protection regulation: a critical perspective." *Journal of Risk Research* (2019): 1-14.

Huang, Guo-hua; Niu, Xiongying; Lee, Cynthia; and Ashford, Susan J. "Differentiating cognitive and affective job insecurity: Antecedents and outcomes." *Journal of Organizational Behavior* 33, no. 6 (2012): 752-769.

Kohn, Rita S. "The Model Contract." *Ent. & Sports Law.* 11 (1993): 9.11

Krausz, Michael. *Managing information security breaches: studies from real life*. IT Governance Publishing, 2015.

Manro Rajan; Randhawa, Rajneesh; and Joshi, A. "Security Issues in Cloud based e-Governance model." *International Journal of Computers & Distributed Systems* 1, no. 1 (2012).

Porcedda, Maria G. "Patching the patchwork: appraising the EU regulatory framework on cyber security breaches" (2018) Computer Law & Security Review 34, no. 5, 1077-1098

Romanosky, Sasha; Hoffman, David; and Acquisti, Alessandro. "Empirical analysis of data breach litigation". (2014) Journal of Empirical Legal Studies. 74-104

Romanosky Sasha; Sharp, Richard; Alessandro Acquisti, "Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal". (2010), Article presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard University, Cambridge, MA

Romanosky, Sasha; Telang, Rahul; Acquisti, Alessandro. "Do data breach disclosure laws reduce identity theft?" (2011) Journal of Policy Analysis and Management, 256-86

Skinner, Timothy H. "California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation." *Rich. JL & Tech.* 10 (2003).

Whitman, M. E. & Mattord, H. J. *Principles of Information Security* (Cengage Learning, 6th edn, 2018)

Whitman, M. E. & Mattord, H. J., *Principles of Information Security*. (Thompson Course Technology, 3rd ed, 2009).

Wood, C. "Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature" (2004) Computer Fraud & Security 2004, no.1.

## Chapter 2: Africa's Multilateral Legal Framework on Personal Data Security: What Prospects for the Digital Environment?

Published in *International Conference on e-Infrastructure and e-Services for Developing Countries*, pp. 38-58. Springer, Cham, 2019

**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 compared to the EU data protection regime, 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, digital environment, African Union, ECOWAS

## 2.1 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 4 million by 2000, and the Information Technology Union (ITU) estimates 781 million mobile phone subscriptions in the continent in 2018[99]. Africans are increasingly using the Internet for information society goods and services, ranging from online banking to social networking[100]. 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.[101] Mobile banking has also been on the rise in the continent for close to a decade now,[102] 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[103]. 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[104] is also on the rise, with an estimated 29 billion connected objects by 2022 [105]; 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'[106]. 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,

---

[99] 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

[100] Adesugba Adesoji. "Mobile technology, social media and 180 million people." *J Bus Adm Manag Sci* 6 (2017): 82-5.83. Also David Kayisire & Jiuchang Wei. "ICT adoption and usage in Africa: Towards an efficiency assessment." *Information Technology for Development* 22, no. 4 (2016): 630-653. 641

[101] Andrew Harris, Seymour Goodman & Patrick Traynor. "Privacy and security concerns associated with mobile money applications in Africa." *Wash. JL Tech. & Arts*, *8*, (2012). 245. 246

[102] Gérard Tchouassi. "Can Mobile Phones Really Work to Extend Banking Services to the Unbanked? Empirical Lessons from Selected Sub-Saharan Africa Countries." *International Journal of Developing Societies* Vol. 1, No. 2, (2012) 70-81.71

[103] GSMA, *The Mobile Economy Report 2013* (A.T. Kearney: London, United Kingdom, 2013) p.3

[104] Defined by Peter Stuckmann, & Rainer Zimmermann in: "European research on future internet design." *IEEE Wireless Communications* 16, no. 5 (2009): 14-22, 15 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

[105] Ericson Mobility Report, June 2017. Retrieved from https://www.ericsson.com/en/mobility-report/internet-of-things-outlook. Accessed 26th June 2019.

[106] Madakam Somayya, R. Ramaswamy, and Siddharth Tripathi. 'Internet of Things (IoT): A literature review.' *Journal of Computer and Communications* 3, no. 05 (2015): 164.165

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[107].

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[108] 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[109]. Just as was the case in Europe with the advent of computer processing in the 1970s culminating in the adoption of the Council of Europe's Convention 108[110] and later the EU Directive 95/46/EC[111] on October 24, 1995 [112], 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[113] 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[114] and personal data security. However, national personal data security initiatives are beyond the scope of this paper, which seeks to examine Africa's multilareral legal frameworks on personal data protection with a view of assessing whether they provide

[107] Pier Luigi Emiliani & Constantine Stephanidis. "Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities." *IBM Systems Journal* 44, no. 3 (2005): 605-619. 606

[108] Uchenna Jerome Orji. "Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?" *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. 2015. pp. 105-118.106. IEEE. .Also Uchenna Jerome Orji. 'The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability.' *Masaryk UJL & Tech., 12*. (2018). 91-129. 92.

[109] See generally Seymour Goodman & Andrew Harris. 'The coming African tsunami of information insecurity.' *Communications of the ACM, 53*(12). (2010). 24-27.

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

[111] 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.

[112] Gloria Gonzalez Fuster. *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16). Springer Science & Business. (2014).28 et seq. Also see Orla Lynskey. *The foundations of EU data protection law*. Oxford University Press, 2015.3

[113] Economic Community of West African States

[114] See generally Cynthia Rich. "Privacy laws in Africa and the Middle East." *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA*. (2015).

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.

### 2.2 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.

#### 2.2.1 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[115]. The first internationally-established conceptualisation of the term 'personal data' was enshrined in the OECD[116] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980.

[115] For a discussion on the interchangeability between 'personal data' and 'personally identifiable information', see Paul Schwartz & Daniel Solove. 'The PII problem: Privacy and a new concept of personally identifiable information.' *NYUL rev.* 86 (2011): 1814-1894

[116] The Organisation for Economic Cooperation and Development

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.*'[117] 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[118]. 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 by adopting a definition which calls for a very wide interpretation of what could constitute personal data, in order to cover all "shadow zones" within its scope.[119]

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 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*

[117] 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))
[118] Nadezhda Purtova. 'The law of everything. Broad concept of personal data and future of EU data protection law.' *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.48-56
[119] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal* Data (Adopted on 20th June 2007). p.5

*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.

### 2.2.2 Personal Data Protection

Hustinx maintains that personal data protection (in light of the objective of the Council of Europe's Convention 108) 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.[120] 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[121]. 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.[122] In Europe, with the human right to private life (of the home and correspondences)[123] 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.[124] 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 seeks to reinforce online trust i.e. making individuals feel confident and safe to

[120] Peter Hustinx. '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*, 1-12. (2013).
[121] See the OECD Privacy Framework. Retrieved from http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 2/11/2019. Page 20
[122] Daniel Solove. "The New Vulnerability: Data security and personal information." In Chander, A., Gelman, L., & Radin, M. J. (2008). *Securing privacy in the Internet age*. Stanford University Press. (2008).112
[123] Article 8 of the European Convention on Human Rights of 4 November 1950
[124] Paul de Hert & Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Re-inventing data protection?* (pp. 3-44). Springer, Dordrecht. (2009). 5-6.

share their personal data. Prior to the post-2010 data protection law reforms in the EU and US, the 'notice and consent' model, which consisted of purpose specification, use limitation and 'informed, freely-given' consent was relied on to protect individuals' personal data[125]. After 2010, following established shortcomings of this model like, inter alia, the processing of data by third parties who were not in any direct relationship with individuals, decision or notice fatigue[126]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 responsible and trustworthy use of personal data.[127] 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…'[128] 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[129] [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.

---

[125] Alessandro Mantelero, "The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics." *Computer Law & Security Review* 30, no. 6 (2014): 643-660. 644

[126] See Malin Olivia Soeder. "Privacy Challenges and Approaches to the Consent Dilemma." (Masters thesis). Available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442612* Retrieved 7/11/2019).pp 25 et seq

[127] 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

[128] 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

[129] Orla Lynskey. *The foundations of EU data protection law*. 2015. supra. 46.

- 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.[130]

### 2.2.3 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.

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 & Mattord add Accuracy, Authenticity, Utility and Possession to the list of data security features.[131]

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…" [132] . 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[133] [18].

---

[130] See Article 5, GDPR

[131] Michael E. Whitman & Herbert J. Mattord, *Principles of Information Security*. Cengage Learning, 6th edn. 2018. pp 15-18

[132] 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)

[133] Daniel Solove. "The New Vulnerability: Data security and personal information." (2008). supra. 114

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[134] is still to receive substantial media attention and legal interpretation in Africa, which may raise concern 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.

### 2.3 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.

#### 2.3.1 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[135]. This inadequate cybersecurity response has eased the infection of a huge number of computers in Africa with malware: reportedly over 80% by 2010[136]. 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[137].

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

---

[134] See Graham Greenleaf. "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 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035. Accessed 11th October 2019

[135] 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].

[136] Franz-Stephan Gady, "Africa's cyber Wmd". *Foreign Policy*. Available at *https://foreignpolicy.com/2010/03/24/africas-cyber-wmd/* Published 24th March 2010. Accessed 3rd September 2019.

[137] Seymour Goodman & Andrew Harris. "The coming African tsunami of information insecurity."(2010). supra. 27.

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,[138] 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.

### 2.3.2 Relatively weak privacy culture in Africa

Privacy as a philosophical or even legal phenomenon has not yet received mainstream attention in Africa.[139] Some commentators even advocating that privacy is of little value in the continent, overshadowed by the collectivist lifestyle which is dominant in local African communities[140], advocated as one of the principal features of the traditional African philosophy generally referred to as *Ubuntu*[141]. 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'[142]. Bakibinga also advances the argument that Africans may generally be said to suffer from 'privacy myopia' i.e. the tendency to undervalue the bits of information about themselves so that it does not seem worth it to go to the trouble of protecting such information[143]. It should be pointed out however that this view is not predominant among scholars: Makulilo for example argues that Western influence and globalization has wrought individualism in African urban areas, and privacy is becoming an evolving concept in the continent.[144] Nevertheless, on the other hand, strong notions of privacy arose in Europe since the end of the Second

---

[138] Wayne Dalton, Joey Jansen van Vuuren, and Justin Westcott. "Building Cybersecurity Resilience in Africa." In *12th International Conference on Cyber Warfare and Security 2017 Proceedings*. *Reading: Academic Conferences and Publishing International Limited*. 2017, pp.112-20.118

[139] Alex Makulilo. 'The context of data privacy in Africa.' In *African Data Privacy Laws*. Springer, Cham. (2016). 3-23. 4

[140] Alex Makulilo. 'Privacy and data protection in Africa: a state of the art.' *International Data Privacy Law 2.3,* (2012): 163-178.171

[141] For an elaboration of the concept of *Ubuntu* in African communities, see Nkonko Kamwangamalu."Ubuntu in South Africa: A sociolinguistic perspective to a pan-African concept." *Critical Arts* 13, no. 2 (1999): 24-41.

[142] Olinger, Hanno N., Johannes J. Britz, and Martin S. Olivier. "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa." *The International Information & Library Review* 39, no. 1 (2007): 31-43.13

[143] Cited by Alex Makulilo. ""One size fits all": Does Europe impose its data protection regime on Africa?." *Datenschutz und Datensicherheit-DuD* 37, no. 7 (2013): 447-451.450

[144] Alex Makulilo. "A Person Is a Person through Other Persons-A Critical Analysis of Privacy and Culture in Africa." *Beijing L. Rev.* 7 (2016): 192.194

World War. And while this, since the 1970s, led to advocacy for even stronger personal data protection requirements for companies processing personal data in Europe, the absence of a strong notion of privacy in Africa weakens the grounds for any advocacy for personal data protection.[145]

This situation is not so static though: most African national constitutions do guarantee a right to privacy[146], 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[147]. 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.[148]

### 2.3.3 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.[149] Adejumobi observes that accountability towards their citizens, unfortunately, is generally not a very popular governance option among African governments[150], and Goodman & Harris observe that many of them demonstrate a willingness to operate outside the rule of law and with little accountability[151]. The absence of accountability provides favourable 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

[145] Seymour Goodman & Andrew Harris, supra, 27

[146] 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.

[147] See generally Cynthia Rich. "Privacy laws in Africa and the Near East." *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA*. (September 2017). Also Cynthia Rich. "Privacy laws in Africa and the Middle East."(June 2015).supra

[148] Andrew Harris, Seymour Goodman & Patrick Traynor. "Privacy and security concerns associated with mobile money applications in Africa."(2012). supra. 245. 249

[149] 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.

[150] Said Adejumobi. "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)

[151] Seymour Goodman & Andrew Harris. "The coming African tsunami of information insecurity."(2010). supra. 27.

accountability towards their citizens[152]. In the same light, Banisar 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[153]. Even more concerning is the fact that the technical development and operation of these ID card schemes are franchised to foreign companies[154] which could make claims against privacy violations difficult in terms of jurisdictional conflict

Mass surveillance is equally another issue: Sutherland posits that African governments are extremely reticent to have any accountability or transparency of their interception and surveillance activities.[155] 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

[152] Lukman Adebisi Abdulrauf, & Charles Manga Fombad. "The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?" (2016). Retrieved from http://hdl.handle.net/2263/60613. Accessed 3/10/2019. Page 5

[153] David Banisar,"Linking ICTs, the right to privacy, freedom of expression and access to information." *East African Journal of Peace & Human Rights* 16, no. 1 (2010).124. 126

[154] Ibid

[155] Ewan Sutherland, "Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance." *LINK Centre, University of the Witwatersrand.* (2018).1

processing of their personal information and, in the process, ensure a trustworthy and secure online environment for the flow of personal data.

## 2.4 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.

### 2.4.1 The ECOWAS[156] Data Protection Act

ECOWAS is the main interstate organization of Western Africa with fifteen members,[157] established by the Treaty of Lagos on 28th May 1975[158]. Article 3 (2) (a) of the 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[159] . 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.[160]

---

[156] 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)

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

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

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

[160] Paragraphs 8-11, Preamble, ECOWAS Data Protection Act

### 2.4.2 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 materialising 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.[161] 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.[162]

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 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)).

### 2.4.3 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.

#### 2.4.3.1 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

[161] Alex Makulilo, "Myth and reality of harmonisation of data privacy policies in Africa." *Computer Law & Security Review*31, no. 1 (2015): 78-89. 81

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

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).

#### 2.4.3.2 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]'[163]. 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.[164]

[163] Peter Hustinx. "The role of data protection authorities." In *Reinventing Data Protection?*, pp. 131-137. Springer, Dordrecht, 2009. 133

[164] 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

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.

#### 2.4.3.3 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[165], 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.

## 2.5 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.

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

### 2.5.1 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[166], and has been taken up by other states and jurisdictions, including the European Union (first by the e-Privacy Directive[167] in 2002, and later the EU GDPR[168] 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'[169]. 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[170]. 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[171] . It also ensures accountability of the data controller in data processing, which requires controllers to be able to actively demonstrate compliance to personal data protection rules at any time, and typically without waiting on data subjects or supervisory authorities to point out shortcomings.[172]

This measure 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

[166] Gina Marie Stevens. "Data security breach notification laws." *Congressional Research Service* (2012).
[167] 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)
[168] Article 33
[169] European Commission, Commission Staff Working Paper SEC (2012) 72 final. Impact Assessment Accompanying the General Data Protection Regulation (2012)) p.100
[170] Samson Esayas. "Breach Notification Requirements under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance,." *J. Marshall J. Info. Tech. & Privacy L.* (2014) 317. 322-323
[171] See generally Paul Schwartz & Edward J. Janger. "Notification of data security breaches." *Mich. L. Rev., 105,* (2006).913.
[172] Philippe Boillat & Morten Kjaerum. "Handbook on European data protection law." *Luxembourg: Publications Office of the European Union* (2014).77

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.

### 2.5.2 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 [173]. 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.[174]

As Cunningham notes, regulations protecting privacy and personal information could simultaneously encourage data security – as well as incentivise those entities that provide data security[175]. 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 [176]. These also include techniques like encryption, anonymisation or pseudonymisation [177]. 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

[173] See for example Paragraph 44, EU Article 29 Working Party. "The future of privacy", WP 168, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf, adopted 1 December 2009

[174] 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.

[175] McKay Cunningham. "Privacy in the age of the hacker: balancing global privacy and data security Law." *Geo. Wash. Int'l L. Rev.* (2012) 45. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138307. Accessed 5/10/2019.

[176] Rolf H. Weber. "Internet of things: Privacy issues revisited." *Computer Law & Security Review* 31, no. 5 (2015): 618-627. 621

[177] See Europa, Privacy Enhancing Technologies (PETs) available at http://europa.eu/rapid/pressrelease_MEMO-07-159_en.htm, dated 2 May 2007. Accessed 24/2/2019

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.[178]

### 2.5.3 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 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 scholars as a risk-management kind of legal regime[179].

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."[180] Similar to the principle of confidentiality and security of processing discussed in Section 3 above, the European approach is much more explicit and lays down guidelines to prove

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

[179] For a discussion of risk management in data protection law, see generally Raphael Gellert. "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 (2016): 481.

[180] Also see Article 32 GDPR

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.

### 2.5.4 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[181]. 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 or data protection certification could aid compliance, 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[182]. Benefits of privacy seals may also include: generation of privacy and data protection accountability and oversight; enhancement of trust and confidence, reputational, competitive and market advantages to entities using them; generation of privacy awareness; assistance in proving fulfilment of privacy and data protection obligations[183].

### 2.5.5 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

[181] See generally Rowena Rodrigues, David Wright & Kush Wadhwa. "Developing a privacy seal scheme (that works)." *International Data Privacy Law* 3, no. 2 (2013): 100-116.
[182] See for example Recital 100 GDPR, which encourages the establishment of personal data protection certification seals and schemes.
[183] Rowena Rodrigues, David Barnard-Wills, Paul De Hert, and Vagelis Papakonstantinou. "The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR." *International Review of Law, Computers & Technology* 30, no. 3 (2016): 248-270. 249.

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.

### 2.5.6 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[184], 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 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.

## 2.6 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

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

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 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. However, they 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 (the 1995 Directive and the 2016 GDPR), 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, compared to the EU response, some significant security mechanisms are missing from both instruments, including provisions for data breach notification, Data Protection by Design, use of privacy certification schemes or the establishment of a direct liability relationship between the data controller and data subjects. These omissions, it is suggested, could be addressed by the adoption of additional protocols modifying these instruments, or in future multilateral texts to ensure relatively strong data security standards for African citizens, and promote a trustworthy and safer digital environment.

**References for Chapter 2**

Abdulrauf, L.A., & Fombad, C.M. "The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?" (2016). Retrieved from http://hdl.handle.net/2263/60613.

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)

Adesoji, A. "Mobile technology, social media and 180 million people." *J Bus Adm Manag Sci* 6 (2017): 82-5

Banisar, D. "Linking ICTs, the right to privacy, freedom of expression and access to information." *East African Journal of Peace & Human Rights* 16, no. 1 (2010).124

Boillat, P. & Kjaerum, M. "Handbook on European data protection law." *Luxembourg: Publications Office of the European Union* (2014).

Cunningham, M. "Privacy in the age of the hacker: balancing global privacy and data security Law" *Geo. Wash Int'l L. Rev* (2012). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138307

Dalton, W., van Vuuren J.J & Westcott, J. "Building Cybersecurity Resilience in Africa." In *12th International Conference on Cyber Warfare and Security 2017 Proceedings. Reading: Academic Conferences and Publishing International Limited*. (2017).112-20.

De Hert, P. & Gutwirth, S. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Re-inventing data protection?* (pp. 3-44). Springer, Dordrecht. (2009)

Emiliani, P.L. & Stephanidis, C. "Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities." *IBM Systems Journal* 44, no. 3 (2005): 605-619.

Esayas, S. "Breach Notification Requirements under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance." *J. Marshall J. Info. Tech. & Privacy L.* (2014) 317

Ericson Mobility Report, June 2017. Retrieved from https://www.ericsson.com/en/mobility-report/internet-of-things-outlook. Accessed 26th June 2019.

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

Fuster, G. G. *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16). Springer Science & Business. (2014).

Gady, F.S. "Africa's cyber Wmd". *Foreign Policy*. Available at *https://foreignpolicy.com/2010/03/24/africas-cyber-wmd/* Published 24th March 2010. Accessed 3/9/2019.

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 (2016): 481.

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 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035. Accessed 11th October 2019

Goodman, S. & Harris, A. "The coming African tsunami of information insecurity." *Communications of the ACM, 53*(12). (2010). 24-27.

Goodman S., Harris, A. & Traynor P. "Privacy and security concerns associated with mobile money applications in Africa." *Wash. JL Tech. & Arts, 8*, (2012). 245.

GSMA. *The Mobile Economy Report 2013* (A.T. Kearney: London, United Kingdom, 2013)

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*. (2013).1-12.

Hustinx, P. "The role of data protection authorities." In *Reinventing Data Protection?*, pp. 131-137. Springer, Dordrecht. (2009).

Kamwangamalu, N. "Ubuntu in South Africa: A sociolinguistic perspective to a pan-African concept." *Critical Arts* 13, no. 2 (1999): 24-41.

Kayisire D. & Wei, J. "ICT adoption and usage in Africa: Towards an efficiency assessment." *Information Technology for Development* 22, no. 4 (2016): 630-653.

Lynskey, O. *The foundations of EU data protection law*. Oxford University Press. (2015)

Makulilo, A. "A Person Is a Person through Other Persons-A Critical Analysis of Privacy and Culture in Africa." *Beijing L. Rev.* 7 (2016): 192

Makulilo, A. "Myth and reality of harmonisation of data privacy policies in Africa." *Computer Law & Security Review*31, no. 1 (2015): 78-89

Makulilo, A. "'"One size fits all": Does Europe impose its data protection regime on Africa?." *Datenschutz und Datensicherheit-DuD* 37, no. 7 (2013): 447-451.

Makulilo, A. “Privacy and data protection in Africa: a state of the art.” *International Data Privacy Law 2.3*, (2012): 163-178.

Makulilo A. “The context of data privacy in Africa.” In *African Data Privacy Laws*. Springer, Cham. (2016). 3-23.

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.” *Computer Law & Security Review* 30, no. 6 (2014): 643-660

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." *The International Information & Library Review* 39, no. 1 (2007): 31-43

Orji, U.J. “Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?” *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. 2015. pp. 105-118.106. IEEE.

Orji, U.J. “The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability.” *Masaryk UJL & Tech., 12*. (2018). 91-129.

Purtova, N. “The law of everything. Broad concept of personal data and future of EU data protection law.” *Law, Innovation and Technology* 10, no. 1 (2018): 40-81

Rich, C. “Privacy laws in Africa and the Middle East.” *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA*. (2015).

Rich, C. “Privacy laws in Africa and the Near East.” *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA*. (September 2017).

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." *International Review of Law, Computers & Technology* 30, no. 3 (2016): 248-270

Rodrigues, R., Wright, D. & Wadhwa, K. "Developing a privacy seal scheme (that works). *International Data Privacy Law* 3, no. 2 (2013): 100-116.

Schwartz, P. & Janger, E.J. “Notification of data security breaches.” *Mich. L. Rev., 105*, (2006). 913

Schwartz, P. & Solove, D. “The PII problem: Privacy and a new concept of personally identifiable information.” *NYUL rev.* 86 (2011): 1814-1894

Soeder, M.O. “Privacy Challenges and Approaches to the Consent Dilemma.” (Masters thesis) (2019). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442612 Retrieved 7/11/2019.

Solove, D. “The New Vulnerability: Data security and personal information.” In Chander, A., Gelman, L., & Radin, M. J. (2008). *Securing privacy in the Internet age*. Stanford University Press. (2008).

Somayya M., R. Ramaswamy, and Tripathi S. 'Internet of Things (IoT): A literature review.' *Journal of Computer and Communications* 3, no. 05 (2015). 164

Stevens, G.M. "Data security breach notification laws." *Congressional Research Service* (2012).

Stuckmann P., & Zimmermann, R. "European research on future internet design." *IEEE Wireless Communications* 16, no. 5 (2009): 14-22

Sutherland, E. "Digital Privacy in Africa: Cybersecurity, Data Protection & Surveillance." *LINK Centre, University of the Witwatersrand.* (2018).

Tchouassi, G. "Can Mobile Phones Really Work to Extend Banking Services to the Unbanked? Empirical Lessons from Selected Sub-Saharan Africa Countries." *International Journal of Developing Societies* Vol. 1, No. 2, (2012) 70-81.

Weber, R.H. "Internet of things: Privacy issues revisited." *Computer Law & Security Review* 31, no. 5 (2015): 618-627

Whitman, M.E. & Mattord, H.J, *Principles of Information Security*. Cengage Learning, 6th edn. (2018).

## Chapter 3: The Effect of Africa's Adoption of the EU Concept of Personal Data: the Case of Examination Results

Published in *2019 IST-Africa Week Conference (IST-Africa)*, pp. 1-13. IEEE, 2019

**Abstract**

European personal data protection standards as set by the Data Protection Directive and recently the General Data Protection Regulation have and are still being copied by African jurisdictions. Under these standards, a broad definition is accorded to personal data, enabling it to cover a wide range of information. The 2017 *Nowak* decision by the European Court of Justice held the scope of personal data to include an examination candidate's evaluated examination script, which by analogy, would include their examination results. Considering European influence on African law, and especially the latter's adoption of almost identical definitions of personal data in its international data protection instruments, examination results would most likely acquire a status of personal data in African case law.

This article argues that while privacy over examination results is fairly respected across African states, a personal data status will further protect Africans by reinforcing their right to information self-determination, and also help shield them from unwanted profiling through Big Data analytics. However, exercising some data protection rights could face some difficulties: the absence of a strong sense of privacy on personal information in Africa, uncertainty of obtaining informed consent for (further) processing of examination results in rural areas, and the difficulty to prove injury in the event of a data breach involving unauthorised access to stored but already published examination results before African courts

**Keywords:** Data protection, Examination results, African Union, ECOWAS, European Union

## 3.1 Introduction

This article adopts a general standpoint that the adoption by Africa of the European concept of personal data under the Data Protection Directive (DPD)[185] of 1995 and its successor the General Data Protection Regulation (GDPR),[186] while promoting information privacy[187] and personal data protection across the continent, could also be faced with some societal and legal hindrances in enforcing the data protection rights of Africans. Focusing on the domain of education, the article aims to illustrate, firstly, that EU influence on African data protection law leads to the interpretative inclusion of academic examination results as personal data under African data protection instruments. Secondly, it argues that while a personal data status on examination results would improve personal data protection in Africa, enforcing its corresponding rights could prove considerably difficult due to socio-cultural and infrastructural realities. In the course of this analysis, the Article also makes a further distinction between privacy rights and personal data protection rights over examination results. In essence, it points out that though African societies have been predominantly described as collectivist with less value on privacy as compared to European societies founded on individualism, a lot has been done across the continent to ensure the confidentiality of examination results. However, a personal data protection status on examination results will raise the latter beyond the mere scope of privacy law, to include further and broader protections essential for guaranteeing the fundamental rights of Africans as the continent continues embracing the Information Society.

European data protection law has been referred to as a hybrid body of laws offering fundamental rights-based protection of personal data while simultaneously favouring aspects of economic regulation[188.] As an instrument of economic regulation, it seeks to harmonize the protection of personal data within regional and (with regard to trans-border data flows) beyond continental borders, thereby removing barriers to the free flow of personal data to international markets for operators who comply with data protection requirements. It has also been hailed as the legal system which currently offers the highest protection for individuals with regard to the processing of their

[185] 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 L 281, 23/11/1995, 0031–0050 (repealed by the General Data Protection Regulation 2016).

[186] 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.

[187] This article adopts Westin's definition of Information privacy, which is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Alan Westin, *Privacy and Freedom,* Atheneum: New York, 1967.p.7

[188] Orla Lynskey, *The foundations of EU data protection law*. Oxford University Press. (2015) 76 – 78. Also see Article 1(3) GDPR which states that "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

digital personal information by private companies or public institutions[189]. And one of the means the European legislators have chosen to attain such protection is, first and foremost, to adopt a very broad material scope of data protection law: personal data[190].

Africa has also been manifesting concerns about the safety and security of online information of its residents, which has culminated in the adoption of the ECOWAS Data Protection Act[191] in 2010 and the African Union Convention on Cybersecurity and Data Protection in 2014. These instruments, with regard to data protection and especially their definition of personal data, are almost wholly copied from EU data protection instruments; which could be commendable, given the esteem in which EU data protection standards are globally held, having been credited with "creating one of the world's leading paradigms for privacy protection, which has served as an inspiration to legal regimes outside Europe"[192]. It should be stressed here that while there has been national responses by many African states over the last decade to personal data protection concerns, with over 25 African states having comprehensive data protection laws to date, this article focuses solely on the ECOWAS and AU instruments, in order to have a widest possible spectrum of the data protection standards in the continent.[193] It is also worth mentioning that academic examination data has also come under the scrutiny of national data protection legislation in Africa. The Ghanaian Data Protection Act of 2012 expressly excludes, from the scope of personal data, marks recorded on an academic or professional examination script for the purpose of determining the examination results.[194] The Act, however, is silent as to whether the ensuing examination results are personal data per se.

The tendency of copying or getting legal inspiration from Europe by African lawmakers to regulate internal affairs, as will be discussed later in this article, is not a new phenomenon. As a matter of fact, a significant section of African literature on data protection so far has been dedicated to a call for the application of EU-inspired data protection legal frameworks within African territories. To cite

---

[189] See Ameesh Divatia."GDPR and the 'Security by Compliance' Mistake", 22nd July 2018. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/02/gdpr-and-the-security-by-compliance-mistake/#1ca90fb5ecc4 Accessed 29 October 2018

[190] For a discussion on the broad nature of the notion of personal data in European data protection law, see Nadezhda Purtova. "The law of everything. Broad concept of personal data and future of EU data protection law." *Law, Innovation and Technology* 10, no. 1, (2018) 40-81

[191] Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, adopted at the 37th Session of the Authority of ECOWAS Heads of State and Government, (Abuja, 16 February, 2010).

[192] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri. Review of the European Data Protection Directive. (Rand Europe, 2009). xiii. Available at https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf Accessed 3/2/2019

[193] The AU Data Protection Convention is not yet effective, and will enter into force upon the deposit of the 15th member state ratification instrument by the Chairperson of the Commission of the African Union, as per the Convention's Article 36. So far (March 2020), there have been only 5 corresponding ratifications and deposits.

[194] Article 72, Ghana Data Protection Act 2012.

a few authors arguing to this effect, Ubena,[195] Kusamotu[196] and Izougu[197] use the 1995 Data Protection Directive as a measuring rod to assess the level of information privacy in Tanzania and Nigeria respectively. What appears to be overlooked by these commentators however is the fact that the material scope of European personal data protection law, through its definition of personal data, could be problematic due to its broad, complex nature which allows for a very vast range of information to fall under personal data protection law, an issue already highlighted by European legal scholars[198]. Such complexity, which has already been the object of litigations at the level of the European Court of Justice[199], could equally be faced by African courts in enforcing due personal data protection rights.

This article accordingly contends that endorsing a status of personal data on examination results as is the case in Europe upholds general personal data protection in Africa, but could encounter applicability and enforceability hindrances within an African context. This introduction shall be followed by a second section which, based on existing literature, shall examine the EU data protection notion of personal data with particular focus on its extensive scope, and how its interpretation points to the inclusion of examination results. This will be followed by a third section which shall present the two main African multinational data protection instruments, discuss their EU-inspired definition of the concept of personal data, and briefly examine the odds of an interpretation of personal data protection standards in African courts similar to their interpretation by the European judiciary. The fourth section discusses the protective advantages of a personal data status on examination results, as well as some setbacks which could be encountered in the enforcement of some these rights in an African context. A fifth section concludes the article.

### 3.2 The (broad) concept of personal data under EU law

Being the centre of the data protection legal machinery, personal data determines the material scope of data protection law as well as, consequently, the scope of two main texts of reference of European

[195] John Ubena. "Tanzania lag on privacy law." *Tanzania Legal News*, published online on 8th June 2010, https://tanlex.wordpress.com/2010/06/08/tanzania-lag-on-privacy-law/ Accessed 28 October 2018

[196] Ayo Kusamotu. "Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46." *Information & Communications Technology Law 16.2* (2007) 149-159.

[197] Chukwuyere Izuogu. Data protection and other implications in the ongoing SIM card registration process. (2010). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665

[198] For a general critique of the broad material scope of EU data protection law, see Nadheza Purtrova, *The Law of Everything*, supra.

[199] The European Court of Justice has entertained a number of cases with the objective of determining whether a given type of dataset is 'personal data' under the 1995 Directive e.g. Joint cases C-141/12 and C- 372/12 YS and M. and S. v Minister of Immigration, Integration and Asylum [2016], ECLI:EU:C:2014:2081, Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994, Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.

data protection law, the 1995 Data Protection Directive (DPD, now repealed) and the GDPR[200]. The data protection process is engaged only when personal data is processed (Article 3(1) DPD and Article 2(1) GDPR), hence its major significance.

Under the GDPR, closely similar to the DPD 'personal data' is defined as:

> '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.'[201]

The broad scope of what could be termed personal data is well expressed in this definition. A very vast range of data categories could fall under this definition, especially in these times characterised by fast-paced, incalculable data processing to meet the demands of today's data-driven society and economy. According to Purtrova: "it has become widely accepted among scholars that as the data processing technologies advance, and the pool of data which can be combined grows, and as combining databases becomes daily practice of intelligence agencies, 'smart city' municipalities, and advertising, so does the reasonable likelihood of somebody being able to link any piece of information to a person."[202] In its quest to offer the best possible protection to information society service users, the EU legislator chose to adopt a definition of personal data which could be stretched, it has been argued, to include virtually everything[203]. As noted by Solove and Schwartz, one benefit of this approach of adopting a broad definition to personal data is that it recognizes the expanding ability of technology to re-identify information and to link scattered crumbs of information to a specific individual[204]. As noted by the Article 29 Working Party[205], the European Commission's original proposal stated that "*as in Convention 108, a broad definition is adopted in order to cover all*

[200] It should be pointed out that although the Data Protection Directive has now been repealed by the General Data Protection Regulation, this does not affect the concept of personal data as it was under the Directive. See the Opinion of Advocate General Kokott [3] in Nowak, ibid.
[201] Article 4(1) GDPR.
[202] Nadezhda Purtova. "The law of everything. Broad concept of personal data and future of EU data protection law."(2018) supra.47
[203] Ibid, Note 49, 66
[204] Paul M Schwartz and Daniel J. Solove. *"*Reconciling personal information in the United States and European Union." *Cal. L. Rev.* 102 (2014). 877.892
[205] The former EU advisory authority on the matters of data protection, composed of national data protection authorities and headed by a European Data Protection Supervisor. Under the GDPR, in force since May 2018, it has been replaced by the European Data Protection Board (EDPB).

*information which may be linked to an individual*", and the Commission's modified proposal noted that "*the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual*"[206]. With the EU approach, it therefore appears *any* information 'concerning' or 'relating to' an individual should be treated as personal data.

### 3.2.1 Information 'relating to'

This aspect of the definition of personal data has been described by the WP29 as 'crucial as it is very important to precisely find out which are the relations/links that matter and how to distinguish them.'[207] In general, information can be considered to "relate" to an individual when it is *about* that individual[208].

In a 2005 Opinion on RFID tags, the WP29 stated that "*data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*."[209] It further establishes that information could "relate to" a person in terms of 'content', 'purpose' or 'result'[210]. 'Content' is satisfied when information is clearly about the person e.g. a patient's medical analysis; 'purpose' 'can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual; and 'result 'is satisfied if the data is likely to have an impact on a certain his/her rights and interests[211]. It was on similar grounds that the European Court of Justice, in 2017, rules examination scripts to be personal data because they 'relate to' a candidate.

### 3.2.2 *Nowak v. Data Protection Commissioner*[212]: Examination scripts (and results?) as personal data

In 2017, a landmark decision was reached in the case of *Peter Nowak v. Data Protection Commissioner*. In 2009, Peter Nowak, a registered student with the Institute of Chartered Accountants of Ireland (CAI) asked to view his scripts for an accounting exam after failing it for the fourth time, with a view to challenging the result. The CAI declined releasing, saying it did not constitute personal data under data protection legislation. Mr. Nowak took his complaint to the Data Protection

[206] Article 29 Working Party Opinion 4/2007 on the concept of personal data, 20 June 2007 ('WP 136').4
[207] WP 136 (Ibid). 9.
[208] Ibid.
[209] WP 136 (Ibid), 10.
[210] Ibid
[211] Ibid, 10-11
[212] Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994

Commissioner, but was rejected on the same grounds as with the CAI. After appealing to the Circuit Court, then the High Court, the case got to the Supreme Court which decided to ask the European Court of Justice for guidance. In its reference for a preliminary ruling, the Irish Supreme Court essentially asked whether the exam script containing the candidate's answers and the examiner's comments regarding those answers might constitute personal data[213]. Both the response by Advocate General of the European Court of Justice (in her Opinion) and the Court were in the affirmative.

The Advocate General's reasoning was consistent with the WP29 approach to consider information as personal data when it is processed with a purpose of evaluating the status or behaviour of an individual. Even though the examination exercises are 'formulated in abstract terms or relate to hypothetical situations',[214] 'the script is a documentary record that that individual has taken part in a given examination and how he performed'[215]. She further states that 'in every case, the aim of an examination […] is to identify and record the performance of a particular individual, i.e. the examination candidate. Every examination aims to determine the strictly personal and individual performance of an examination candidate'[216].

The Court followed the reasoning of the Attorney General. It reaffirmed the notion 'personal data' as potentially encompassing any information, as long as it 'relates' to the data subject[217], stating that the condition is met where the information is linked to a particular person 'by reason of its content, purpose or effect'[218]. Most significant, the Court found that the link between the information and the individual relevant because both the candidate's answers and the examiner's comments relate to the data subject in all three aspects: they reflect the information about the candidate (his knowledge, thought process and, in the case of a handwritten answer, information about his handwriting, as well as the examiner's opinion regarding the candidate's performance)[219]; the purpose of their processing is to evaluate the candidate in terms of his professional abilities; and the use of this information is 'liable to have an effect on his or her interests'[220].

---

[213] *Nowak,* Opinion of Advocate General Kokott [2].
[214] Ibid [19]
[215] Ibid [21]
[216] Ibid [24]
[217] *Nowak,* [34].
[218] Ibid [35]
[219] Purtova (2018) Ibid, 71
[220] *Nowak,* [39]. But see *YS and others* (17th July 2014, ECLI:EU:C:2014:2081) [Paragraph 46] where the ECJ created a precedent to the effect that the right to access a document affecting one's interest is not absolute and may be denied in certain circumstances (in this case, if it will lead to granting access to administrative documents). The Courts usually balance the right of against other fundamental rights and interests, to determine its enforcement. See Antonella Galetta and Paul de Hert. "A European Perspective on Data Protection and the Right of Access." In *The Unaccountable State of Surveillance*, pp. 21-43. Springer, Cham, 2017. p 35.

The above decision lays a European precedent of evaluated examination scripts being considered students' personal data by reason of its purpose and effect. Closely related to evaluated examination scripts are examination results, which are a produce of the evaluated script, are a display of a candidate's skill and abilities in a given area of study, and also have an effect on a candidate's interests (these results will determine whether or not the candidate gets further admission, jobs, and could serve as guide for his career path). By interpretation therefore, examination results, at least within the WP29 interpretation of purpose and result, most certainly fall under personal data under EU law. This view is shared, for example, by the University of Reading in the United Kingdom, which expressly considers examination results as personal data on its Information Management and Policy Services[221].

The following section presents African intergovernmental data protection instruments and their material scope of application which, by interpretation, would include examination scripts and/or examination results.

### 3.3 African intergovernmental data protection legislations

A number of African countries[222], intergovernmental organisations and the African Union as a continental whole have been adopting legal frameworks on personal data protection. The current intergovernmental legal frameworks in Africa with focus on personal data protection are the EAC (East African Community) Framework for Cyberlaws (2008), SADC (Southern Africa Development Community) Model Law on Data Protection (2010), ECOWAS (Economic Community of West African States) Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010) and the African Union Convention on Cybersecurity and Personal Data Protection (2014). With the SADC and EAC legal frameworks being only model laws with no binding legal effect on their member states, this paper shall focus on the ECOWAS and AU legal frameworks which were adopted with the intention of (prospectively) creating legal obligations among member states.

#### 3.3.1 ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection

The Supplementary Act A/SA.1/01/10 on Personal Data Protection within the ECOWAS (hereinafter the ECOWAS Data Protection Act) was adopted during the 37th session of the Authority of ECOWAS Heads of State and Government in Abuja on16 February 2010. In its Preamble, the Act recognizes that

[221] https://www.reading.ac.uk/internal/imps/DataProtection/DataProtectionRequirements/imps-d-p-examinations.aspx (accessed 21st April 2019)

[222] By 2015, 17 African countries had adopted comprehensive personal data protection legislation. See Cynthia Rich. "Privacy laws in Africa and the Middle East." *The Bureau of National Affairs, editor. Privacy and Security law report*. Bloomberg: BNA, (2014).1

technology advancements greatly ease personal data processing and hence bring about unprecedented problems of personal data protection. It also seeks to address problems relating to personal data protection through a harmonized legal framework for data protection within the ECOWAS sub-region.

### 3.3.2 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 (hereinafter the AU Data Protection Convention) provides a legal framework regulating three distinct domains and divided in as many corresponding sections: Electronic commerce, Data Protection and Cybercrime/cybersecurity. Similar to its ECOWAS predecessor but with a continental scope, it has as objective, as regards personal data protection, the establishment of 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[223]. It is not yet binding on member states, and will attain this status upon ratification by 15 member states[224]. So far (March 2020) though, only five member states (Ghana, Guinea, Mauritius, Namibia and Senegal) have ratified the Convention.

### 3.3.3 Defining personal data under both instruments.

Both the above ECOWAS Data Protection Act and African Union Data Protection Convention, like other instruments addressing personal data protection everywhere else, are applicable only when personal data is being processed. In delimiting the material scope, both instruments provide for a definition of personal data. The ECOWAS Data Protection Act states:

> 'Personal data means any information relating to an identified individual or 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'[225].

The AU Data Protection Convention, closely following this approach, states as follows:

> 'Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in

[223] Article 8(1), African Union Convention on Cyber Security and Personal Data Protection
[224] Article 38, ibid
[225] Article 1 Para.5, ECOWAS Data Protection Act

particular by African Union Legal Instrument reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity'[226].

The closeness to the definition of the notion of personal data by European instruments like the 1995 Data Protection Directive is quite obvious in these definitions, with the (vague) terms 'any information', 'relating to', 'identified' and 'identifiable' appearing in all three definitions. As has already been discussed in the preceding section of this paper, these terms allow for a very broad range of data to fall under data protection law, and as such, require protection and processing restrictions in accordance with the said legal framework. And considering that so far there have been no official guidelines produced by these intergovernmental organisations or case law from any intergovernmental African court providing a detailed legal and contextual interpretation of the above definitions of personal data, it is only logical that in applying (and hence interpreting) the above instruments in African courts, reference would most probably be made to European legal opinions and case law to reach a decision as regards the material scope of personal data in Africa.

### 3.3.3 Similar interpretation of personal data in Africa as in the EU: what odds?

It is important to recall here that the prospect of an EU-interpretation of data protection concepts by national African courts is not very unlikely, and this could be attributed to two main reasons advanced by Alex Makulilo[227]. First, not only are African countries steadily adopting data protection laws inspired by EU legislations, most African countries inherited their current legal systems from European countries imposed on them during the colonial era, and are thus no strangers to European legal systems. Actually, most of these countries still rely on case law of their former colonial rulers to address issues which may not have been addressed by national law.[228] Cameroon courts in the common law jurisdiction of the country, for example, still refer to English law in to address areas not covered by national law[229], and still rely on English case law as persuasive authority during court pleadings.

---

[226] Article 1 Para.36, AU Data Protection Convention.

[227] Alex B. Makulilo, "One size fits all: Does Europe impose its data protection regime on Africa?" *Datenschutz und Datensicherheit-DuD* 37.7, (2013) 447-451.451

[228] For example, Kenya being a former English colonial territory and inheriting English common law, Kenyan legal practitioners, still refer to English case law as persuasive authority in Kenyan court. See generally Michael Nyongesa Wabwile. "The Place of English Law in Kenya." *Oxford University Commonwealth Law Journal* 3, no. 1 (2003): 51-80. Similarly, English case law still has persuasive authority in Nigerian courts. See Matthew Enya Nwocha. "Customary law, social development and administration of justice in Nigeria." *Beijing L. Rev.* 7 (2016): 430.433

[229] Ephraim Ngwafor. "Cameroon: The Law Across the Bridge: Twenty Years (1972-1992) of Confusion." *Revue générale de droit* 26, no. 1 (1995): 69-77. 71

Secondly, there is an economic motivation; African data protection legislations are mostly modelled upon the EU Data Protection Directive following the aspiration of African countries to meet the 'adequacy' standard of the European law so as to remain attractive for foreign investments[230], a consequence of the so-called "Brussels Effect"[231]. Interpreting personal data protection and standards in similar lines as in European courts is therefore not very far-fetched for African legislators.

### 3.3.4 Principles and rights related to the processing of personal data (and hence examination results)

The above African instruments, like their European counterparts, list a number of principles regulating the processing[232] of personal data, while according a number of corresponding rights to data subjects to protect their fundamental interests in relation to such processing. The principles are listed in Article 13 of the AU Data Protection Convention and Articles 23 to 28 of the ECOWAS Data Protection Act. They include consent (personal data shall be processed only if data subject gives their consent[233], fairness of processing (personal data should not be processed if such processing would not be fair to the data subject), purpose, relevance and storage (personal data should be processed for a specific purpose and should not be further processed for another purpose incompatible with the original purpose, and should not be stored for longer after that purpose has been attained[234]), accuracy, transparency, confidentiality and security of processing. It follows therefore that upon attaining a status of personal data, examination results shall have to be processed in accordance with all the above principles in most African jurisdictions, especially upon the entry into force of the AU Data Protection Convention.

---

[230] Article 25 of the DPD and now Article 45 of the GDPR restrict data transfers of EU residents to countries which do not have an 'adequate' standard of personal data protection.

[231] Term coined in 2012 by Professor Anu Bradford referring to the persuasive force wielded by EU regulations worldwide, attributed to the size of its consumer base and strength of its regulatory institutions. See generally Anu Bradford. "The Brussels effect." *Nw. UL Rev.* 107 (2012): 1.11

[232] Processing of personal data is defined under the AU Data Protection Convention as "any operation or set of operations which is performed upon personal data, whether or not by automatic means such as the collection, recording, organization, storage, adaptation, alteration, retrieval, backup, copy, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and locking, encryption, erasure or destruction of personal data". Any of these actions carried out on examination results should therefore be in accordance with the Convention's established data processing principles.

[233] This is however subject to a number of exceptions: where processing is in compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority, performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or to protect the vital interests or fundamental rights and freedoms of the data subject (Article 13, AU Dara Protection Convention)

[234] As an exception, personal data may be stored for longer periods for historical, statistics or research purposes (Article 13, Principle 3 (d) AU Data Protection Convention)

### 3.4 Examination results as personal data in Africa: potential pros and applicability hitches

It could be fair to assert that before the emergence of data protection law, if examination results were part of mainstream litigations anywhere, it will probably be as regards their integrity, fairness or authenticity; and hardly about the rights individuals have towards them due to their 'personal' nature. But after the DPD and *Nowak,* EU law now accords a personal data status on examination results, subjecting the latter to data protection law. And this legal novelty may well have been transported into the African legal system with the ECOWAS and AU data protection instruments taking up largely identical definitions of personal data and hence identical material scope of personal data protection law.

The ECJ decision in *Nowak* was groundbreaking in that it granted a data protection right of access to and verification of examination scripts by the candidate on grounds that these evaluations, similar to the test previously laid down in WP 136, 'related to' the candidate in terms of content (content of those answers reflects the extent of the candidate's knowledge), purpose (purpose of collecting those answers is to evaluate the candidate's professional abilities) and result (the chance of entering the profession)[235]. Though the case did not concern examination results *stricto sensu*, it could be safe to assert that the Court's ruling would not be different if this were the case. This is because, just as examination script evaluations, examination results do relate to candidates in terms of content (they contain the candidate's name or student ID number), content (the grades, which are only the end result of the evaluation of his conduct)[236] and result (grades will have an impact on future employment chances, or on how his/her peers and family regard and treat him). In the absence of another test provided within the ECOWAS and AU on how African legal practitioners should interpret and apply the 'relating to' phraseology which features on the definitions of the notion of personal data by both instruments, or any related case law, examination results could therefore be considered as personal data on African soil. While this development could, in theory, endorse new grounds for personal data protection, applying such a right in practice could prove considerably difficult in an African, third world context.

#### 3.4.1 Examination results as personal data: protecting fundamental rights of Africans

This subsection discusses how attributing a personal data status to examination results could help protect the fundamental rights and freedoms of Africans.

[235] Nowak, supra [Paragraphs 37-39]
[236] Ibid [Paragraph 38]

#### 3.4.1.1 Endorsing a right to information self-determination of African residents

One of the founding pillars of personal data protection law is the right to information self-determination, popularised by the reasoning by the German Constitutional Court (*Bundesverfassungsgerichsthof*) in its milestone decision of 15th December 1983[237], also referred to as the Population Census Decision.[238] The Court recognized a right of every citizen to 'information self-determination', founded on the right to the 'free development of one's personality' (otherwise referred to as a personality right), protected by Article 2.1 of the German Constitution. In the same light of the internationally recognized right to self-determination which protects an individual's right to plan or decide freely without being subject to pressure or influence, the right to information self-determination aims to 'preclude a social order in which citizens no longer can know who knows what, when, and on what occasion about them.'[239] The Court was of the opinion that if citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, or know who may have access to this information, or unsure of whether their dissenting behaviour is noticed or stored, they may be inhibited in exercising their fundamental human rights like freedom of speech or choice.[240]

This reasoning forms the basis and essence of the right to personal data protection, and helps differentiate it with the right to information privacy. The latter is a right enabling an individual choose who is privy to a given piece of information concerning them, which in essence applies only to that piece of information. This means any further information inferred from that original information is apparently not covered by the right to information privacy; though such derived information still relates to the individual and may still significantly affect them.[241] Personal data protection comes in therefore to protect the individual through providing principles, rights and obligations which govern the entire life cycle of the information including inferred information i.e. from the time the information is created, given out, further processed, how further information may be inferred from it, and how this new inferred information is used. In other words, it applies to the individual's information in all its forms. This illustrates that personal data protection includes, but is by no means limited to information

[237] Judgment of 15 December 1983, 1 BvR 209/83, BVerfG 65, 1
[238] Orla Lynskey. *The foundations of EU data protection law* (2015) supra. 94
[239] Antoinette Rouvroy & Yves Poullet. "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy." In *Reinventing data protection?*, pp. 45-76. Springer, Dordrecht, 2009. 49
[240] Gerrit Hornung & Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25, no. 1 (2009): 84-88. 85
[241] For a general discussion on how inferences from personal information affect individuals, see Sandra Wachter & Brent Mittelstadt. "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI." *Colum. Bus. L. Rev.* (2019). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Page 4. Accessed 15th March 2020

privacy. Consent and confidentiality of processing are among the principles of processing listed in the above African data protection instruments which reinforce information privacy, while other principles like fairness, storage and further processing extend individual protections beyond privacy.

Following up on the reasoning in the *Nowak* case, if examination results are representative of the cognitive abilities of an individual in a given area of knowledge (as opposed to another), then such information will be likely to affect them especially in terms of how society judges their intelligence levels. Therefore, giving examination candidates the choice of choosing who views their examination results or limiting the processing of examination results to strictly necessary purposes would ensure that candidates remain reassured against any unfavourable future uses of their results. It should be highlighted here that, in practice, examination candidates already enjoy privacy rights vis-à-vis their examination results. Most West African countries like Nigeria, Ghana, Gambia and Sierra Leone, through the policy of the West African Examinations Council (WAEC), make public examination results privy only to examination candidates, accessible online after relevant identification[242]. Other African countries which make examination results private and confidential include Kenya, Uganda, Zimbabwe, Congo (Brazzaville). In South Africa, university entrance exams (popularly known Matric exams) are published in newspapers but only with the candidates' exam numbers, to maintain anonymity.[243] This is however not the case in all African countries. In Cameroon for example, results of the nationwide secondary school leaving examinations in the country are made available to the general public with no little or no efforts in terms of privacy or anonymity for candidates. The results of Anglophone General Certificate of Education (GCE, organised by the GCE Board) with the full names and grades of candidates, are still made available in some national newspapers the Board's website (www.cameroongceboard.com) with no indicated availability limit, while the results of the *Francophone Baccalauréat de l'enseignement sécondaire* (organised by the *Office du Baccalauréat*) are made read over the radio. Though this eases communication of results, it raises data protection concerns in terms of confidentiality of personal information, for it can never be certain who gets and stores these results. Also, the country's oldest and most popular university, the University of Yaounde, makes some semester examination results (with the full name of candidates, registration number and course examination score) available online on the university's website (www.univ-yaounde2.org) for public consultation and for an undeterminable period of time. Moreover, the trend in recent years has

[242] For example, WAEC offers an online results-checker on www.warcdirect.org, accessible by candidates after inserting their unique registration number

[243] See Tom Head. "Matric results: What time they get released, and when you can collect them" (News Article. Published 7th January 2020) Available at https://www.thesouthafrican.com/lifestyle/when-matric-results-released-what-time-tuesday-7-january-2020/ Accessed 18th March 2020.

been the franchising of the results to foreign-owned private telecom companies, like the French-owned telecom company Orange Cameroon for the *Baccalauréat* results and the South African-owned telecom company MTN Cameroon, so candidates can directly consult their results on their mobile phones against a fee. While this further eases results accessibility for candidates, it should be pointed out that at no point during the examination registration process are the candidates requested to indicate whether or not they consent to the transfer or processing of their results by these private enterprises. Also, with currently no functional personal data protection law in the country, there is no clear legal regime preventing any unfair further processing of these results (in terms of purpose specification, use or storage limitation, transfer of inferred information) by these enterprises for their own profits.

Considering that examination results are directly representative of the cognitive abilities of an individual, it can be argued, as in *Nowak*, that they could have considerable impact on the individual and deserve some appropriate level of regulatory protection. And though a good number of African countries ensure the information privacy of examination results, this right protects only consent and confidentiality of processing (divulgation being part of processing[244]), and does not cover other aspects like purpose specification, storage limitation or fairness of processing. Raising examination results to the status of personal data in African countries shall therefore not only trigger the need for confidentiality in publishing results as is the case in Cameroon, but shall also prompt an all-round and more complete protection of examination results in African countries, limit unfair exploitation by public authorities or private enterprises and further guarantee a right to information self-determination of Africans

#### 3.4.1.2 Curbing Big Data concerns

Examination results, like all pieces of information, form part of the huge universe of (big) data, and could also be part of the data mined by companies and other institutions to classify people under certain profiles of particular skillsets, characteristics or preferences. As Hilderbrandt notes, because this profiling is usually paid for by companies and other data processing institutions, these classifications will be done in line with their interests as opposed to individuals' interests[245]. Such classifications have been documented to pose serious privacy risks, especially in terms of discrimination based on automated-decision making[246]. Wachter and Mittelstadt also observe that Big Data analytics and artificial intelligence draw on highly diverse data of currently unpredictable value,

[244] See note 50

[245] Mireille Hildebrandt. "Defining profiling: a new type of knowledge?." In *Profiling the European citizen*, pp. 17-45. Springer, Dordrecht, 2008. 18

[246] Laura Carmichael, Sophie Stalla-Bourdillon & Steffen Staab. "Data mining and automated discrimination: a mixed legal/technical perspective." *IEEE Intelligent Systems* 31, no. 6 (2016): 51-55.

and correlate them in order to create new value in terms of inferences and predictions about the behaviours, preferences, and private lives of individuals; a trend which could create new opportunities for discriminatory, biased, privacy-invasive profiling and decision-making[247]. Algorithms could misclassify or misjudge an individual following an automated-decision making process, and such errors may disproportionately affect certain groups of people[248]. Because there is no limit to what data could be mined for profiling purposes, nothing eliminates published examination results from the pool of raw, big data which data mining entities dive in to collect elements from which to filter new information to satisfy their interests.

This will imply, for example, that an algorithm tasked by a health institution to fish for persons with potential skills in the field of health will, without prejudice to other combined datasets, place in a favourable position individuals who had better scores in healthcare-related subjects in a public examination. And without any human intervention in such a process, this could be highly discriminatory for individuals who may have healthcare-related skills but for some reason did not perform well in those examinations. Or there could arise situations where people who perform better in management-related courses in university are automatically favoured by data mining algorithms to get loans than those who performed poorly. Attaching a personal data status to examination results could help prevent such outcomes by permitting individuals to decide who to share their examination results with, or whether or not they want their results to be part of the big data universe at all, hence limiting their access or availability, and generally contributing to protection against harms which may befall them through any eventual misuse of these results. This could take the form of exercising relevant data protection rights on examination results like consent before publication in newspapers (as is the case with Cameroon) invoking the storage limitation obligation of the data controller (Article 13, AU Data Protection Convention) or exercising a right to erasure (Article 19 AU Data Protection Convention) to have examination results erased from publicly accessible databases like online portals.

### 3.4.2 Examination results as personal data in Africa: applicability limitations

This subsection discusses the practical difficulties in enforcing data protection rights on examination results upon the latter attaining a status of personal data in Africa.

[247] Sandra Wachter & Brent Mittelstadt. "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI." (2019) supra. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Page 4. Accessed 15/03/2020.
[248] Frank Pasquale. *The black box society: The Secret Algorithms that control Money and Information.* Harvard University Press, 2015.

#### 3.4.2.1 Absence of a privacy awareness in Africa

Faced with constant political conflicts and economic problems, privacy hardly makes top priority on the agenda of African national or regional governments. Even as a legal phenomenon, not much has been written on the right to privacy by African scholars[249]. This has been said to be due to the dominant collectivist and communal lifestyle in local African communities[250] referred to as *Ubuntu*[251]. As a matter of fact, the right to privacy is absent among the basic human rights listed under the 1981 African Charter on Human and People's Rights (ACHPR). Olinger et al suggest that this omission could be due to the fact that privacy was simply not regarded as a necessary right for Africans to live freely and peaceably'[252] Makulilo, however, argues the contrary, observing that Western influence and globalization gradually promotes individualism in urban areas in Africa, and privacy is gradually surfacing as a concept in the continent.[253] Also, most African constitutions today do provide for a right to privacy[254], and as discussed above, African governments have been promoting privacy protection through personal data protection laws. This notwithstanding, there still is a significant lack of privacy awareness among the average population, which weakens grounds for any cultural awareness to support the promotion for personal data protection rights,[255] especially considering the relationship between information privacy and personal data protection (i.e. both aim to protect personal information). It may even be argued that African states employed the use of online resources to communicate examination results to candidates not because there was any wave of a sense of privacy sweeping through the continent, but rather to take advantage of the advent of the Internet to ease access the results for candidates.[256]

---

[249] Alex Makulilo. 'The context of data privacy in Africa.' In *African Data Privacy Laws*. Springer, Cham. (2016). 3-23. 4

[250] Alex Makulilo. 'Privacy and data protection in Africa: a state of the art.' *International Data Privacy Law 2.3*, (2012): 163-178.171

[251] For an elaboration of the concept of *Ubuntu* in African communities, see Nkonko Kamwangamalu."Ubuntu in South Africa: A sociolinguistic perspective to a pan-African concept." *Critical Arts* 13, no. 2 (1999): 24-41.

[252] Olinger, Hanno N., Johannes J. Britz, and Martin S. Olivier. "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa." *The International Information & Library Review* 39, no. 1 (2007): 31-43.13

[253] Alex Makulilo. "A Person Is a Person through Other Persons-A Critical Analysis of Privacy and Culture in Africa." *Beijing L. Rev.* 7 (2016): 192.194

[254] E.g Article 12 of the 1996 Constitution of Cameroon, Article 26 of the 1994 Constitution of the Federal Democratic Republic of Ethiopia, Article 36 of the 1989 Constitution of the Federal Republic of Nigeria.

[255] Seymour Goodman & Andrew Harris. 'The coming African tsunami of information insecurity.' *Communications of the ACM*, *53*(12). (2010). 27

[256]See for example Joseph R. Oppong. "Innovation, science and technology: regional networks for research and technology development in Africa." *Contemporary Regional Development in Africa* (2016): 159, 170, on the Kenyan government allowing exam results online which led to an increase in demand for broadband internet connection in the country.

The lack of a privacy culture influences the lack of awareness for the protection of individuals vis-à-vis their examination results in Africa. This is similar to what Bakibinga terms 'privacy myopia' in Africa i.e. the tendency for Africans to undervalue the bits of information about themselves so that it does not seem worth it to go through the trouble of protecting such information[257]. After their divulgation to various candidates, examination results are generally hardly subject to much public or legal interest any longer. Once results are known, no one seems to care about any further rights which may accrue to them, the only estimated use of their further storage being for the verification of the authenticity of certificates.

#### 3.4.2.2 Getting informed consent for further processing.

As discussed in Section 3.5, personal data protection law generally prohibits the further processing of personal data if such processing is incompatible with the original purpose of processing. However, further processing may be allowed if, among other exceptions listed in the AU and ECOWAS data protection instruments[258], the data subject gives their express consent to the processing. So if examination results do constitute personal data, then any further processing should apparently be subject to the express consent of the candidate or, if he/she is a minor, the consent of their parents. An example of such further processing could be the forwarding of examination results to third parties for prospections of further educational opportunities (e.g. by universities or professional schools searching for new students), scholarship considerations or inclusion into talent pools.

The principal issue here would be determining whether or not such consent is valid or informed[259]. This is because in the first place, the great majority of candidates of public examination results are minors below 21 years of age, and who therefore cannot give valid consent as regards the publication of their examination results. Also, seeking such consent from parents will prove very difficult for two reasons: in the first place, the parents will have to be contacted in person, because to date, most public examination registration procedures in many African countries are done manually and not online. And because these education boards are usually located in urban cities, requiring parents to travel from the far and wide to grant consent for the publication of their children's results just seem too cumbersome and very complex to realise; nor for the Boards to have to recruit and send agents to each candidate's parents to get such consent. Also, a reported 38% of the African adult

[257] Cited by Alex Makulilo. ""One size fits all": Does Europe impose its data protection regime on Africa?." *Datenschutz und Datensicherheit-DuD* 37, no. 7 (2013): 447-451.450

[258] See Article 31 ECOWAS Data Protection Act, Article 13 AU Data Protection Convention

[259] Article 1 of the AU Data Protection Convention defines a data subject's consent to mean "any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing."

population is uneducated[260] which means even if the parents or guardians are contacted, obtaining clear, unequivocal consent might not be evident because it could be difficult to prove that they clearly understand what they are signing up for on behalf of their children.

#### 3.4.2.3 Breach of examination results: grounds for private/class action in damages?

Security of processing is one of the core principles of personal data processing, with data controllers and processors are generally required to take appropriate measures to protect personal data against, among others, accidental destruction and unauthorized disclosure or access[261]. These obligations equally manifest in the AU and ECOWAS data legislation instruments[262]. It therefore follows that upon examination results attaining the status of personal data in Africa (which they apparently are, as has been illustrated above) their processing must be protected from unauthorised access or destruction, and failure to provide such protection amounts to a breach of the controller's legal obligations. This would help ensure data confidentiality and promote much required online trust in a continent progressively enjoying internet penetration and embracing information society trends. However, it also provokes the question as to whether an academic institution or examination board may be sanctioned by a data protection officer or held liable towards a through a private individual or class action for damages by students or examination candidates following a leak of or unauthorised access to academic examination results.

Unauthorised access to a school's database, in the absence of evidence of the contrary, would imply security system in place was not appropriate, which would be a breach of security of processing obligations and could lead to the imposition of a fine among other sanctions by the national Data Protection Authority[263]. However, the question may be asked whether a breach involving unauthorised access to examination results is serious enough to warrant any form of liability in personal damages towards students or examination candidates. Unlike social security numbers which could well be used for identity theft[264], or usernames, passwords or bank account details, breaches of examination results have not been documented as potential data which misuse could harm concerned candidates. However, it should also be mentioned that leaks of personal information have been pointed out to be 'harmful'

[260] http://www.unesco.org/new/en/dakar/education/literacy/ (Accessed 23rd April 2019)
[261] See Article 11 of the OECD Revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines"), adopted on 11 July 2013. Also Article 17, EU Data Protection Directive
[262] Article 43, ECOWAS Data Protection Act, Article 21 AU Data Protection Convention.
[263] Article 12 AU Data Protection Convention
[264] Daniel Solove. "The New Vulnerability: Data security and personal information." In Chander, A., Gelman, L., & Radin, M. J. *Securing privacy in the Internet age*. Stanford University Press. (2008).119

even without a tangible loss to those whose information was leaked: Solove and Keats for example opine that unauthorized access to personal data could cause emotional distress, exposes individuals to a risk of future injury, and causes them to experience anxiety as a result of data breaches compromising their personal data[265]. Nevertheless, in an African context where there is hardly any manifest interest in the use of examination results, especially after divulgation, it may be difficult convincing a judge that a leak of processed examination results could harm or cause distress to an identified or identifiable student or candidate. A candidate may have a case, it can be argued, if the breach involves a complete loss of their results, as this implies the loss of any means to verify the authenticity of their results, which may cost them employment or other academic opportunities for which certificate verifications are mandatory. Such an argument would found a stronger case for harm than mere unauthorized access of the results.

It should be noted that the ECOWAS and AU data protection instruments are currently silent as to any form of direct compensation available to individuals against data controllers and processors for violations of their provisions. Also, apart from South Africa, Kenya and more recently Uganda, there is a significant lack of African case law on privacy[266] which could help determine the scope and relevance of harms related to unauthorised disclosure of personal information like examination results. But considering that the ECOWAS and AU instruments have not classified 'harmless' types of personal data whose leaks are deemed of too trivial consequences, nor have their respective organs produced any guidelines to this effect, unauthorised access to examination results would remain unauthorised access to personal data which, at least from a legal perspective, leaves open the possibility of direct liability and the award of personal damages. Nevertheless, taking cue from Bakibinga's "privacy myopia" which suggestively dominates African societies, lack of privacy case law and little interest shown towards any further use of processing of examination results after publication, it remains very likely that an action for harm due to unauthorized access to stored but already published examination results before an African court may be struck out as irrelevant or trivial.

### 3.5 Conclusion

This article presents a discussion regarding the potential attachment of a personal data status on examination results under African data protection law, inspired by EU case law. In general, it tries to explore how such a development would further consolidate personal data protection rights in Africa

[265] Daniel Solove and Danielle Keats Citron. Risk and Anxiety: A Theory of Data-Breach Harms. *Tex. L. Rev.* 96: (2017) 737. 750

[266] Alex B. Makulilo. "The Future of Data Protection in Africa." In *African Data Privacy Laws*, pp. 371-379. Springer, Cham, 2016.373

through protecting examination results, and also discusses some difficulties which could be encountered with the exercise of data protection rights over examination results in an African context. It engages the discussion first by highlighting the broad material scope of personal data protection law (i.e. personal data), pointing out that its definition by the EU legislator implies that it covers a vast range of information including evaluated examination scripts as was decided by the ECJ in the 2017 *Nowak* case, and which would equally examination results following the reasoning of the judgment. This inclusion of examination results as personal data, it is opined, could also be the case in African case law considering the almost identical definition of personal data in the continent's most popular data protection instruments (the AU Data Protection Convention and ECOWAS Data Protection Act), its adoption of European legal systems introduced in the continent during colonial times, as well as the continual reference, by African legal practitioners, to the case law of European countries to address legal problems.

Based on the above premise, the article then argues that attaching data protection rights to examination results would contribute to consolidating a right to information self-determination of examination candidates. Also, the data protection rights of erasure or storage limitation, if exercised on examination results, would contribute to limiting their availability to a vast number of unknown entities and shield them from any unwanted or discriminatory profiling through Big Data analytics. However, the lack of a strong privacy culture and awareness in Africa, coupled with little manifested interest in the outcome of examination results after their publication could hamper the development of appropriate protection policies. Also, acquiring informed consent from candidates or their parents further processing of their examination results, especially in rural areas, could be challenging since many parents are illiterate and may not fully understand the nature of what they are signing up to. And finally, while a data protection status on examination results would imply the possible liability of the data controller and hence a theoretically possible action for private or class actions by candidates for injury, proving such injury before African courts could be challenging considering the lack of privacy case law in the continent to determine whether unauthorised access to or loss of stored but already disclosed examination could be considered injurious.

**References for Chapter 3**

Bonnici, J.P.M. "Exploring the non-absolute nature of the right to data protection." *International Review of Law, Computers & Technology* 28, no. 2 (2014): 131-143

Bradford, Anu. "The Brussels effect." *Nw. UL Rev.* 107 (2012): 1.11

Carmichael, L., Stalla-Bourdillon, S. & Staab, S. "Data mining and automated discrimination: a mixed legal/technical perspective." *IEEE Intelligent Systems* 31, no. 6 (2016): 51-55.

Divatia, A."GDPR and the 'Security by Compliance' Mistake", 22nd July 2018. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/02/gdpr-and-the-security-by-compliance-mistake/#1ca90fb5ecc4 Accessed 29th October 2019

Galetta, A. & De Hert, P. "A European Perspective on Data Protection and the Right of Access." In *The Unaccountable State of Surveillance*, pp. 21-43. Springer, Cham, 2017.

Goodman, S. & Harris, A. 'The coming African tsunami of information insecurity.' *Communications of the ACM, 53*(12). (2010).

Hildebrandt, M. "Defining profiling: a new type of knowledge?." In *Profiling the European citizen*, pp. 17-45. Springer, Dordrecht, 2008.

Hornung, G. & Schnabel, C. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Review* 25, no. 1 (2009): 84-88

Izuogu, C. *Data protection and other implications in the ongoing SIM card registration process*. (2010). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665

Kusamotu, A. "Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46." *Information & Communications Technology Law 16.2* (2007) 149-159.

Lynskey, O. *The foundations of EU data protection law*. Oxford University Press. (2015)

Makulilo, A. B. "One size fits all: Does Europe impose its data protection regime on Africa?" *Datenschutz und Datensicherheit-DuD* 37.7, (2013) 447-451.

Makulilo, A.B. "Privacy and data protection in Africa: a state of the art." International Data Privacy Law 2.3, (2012): 163-178.

Makulilo, A. B. "The context of data privacy in Africa." In *African Data Privacy Laws* (Springer, Cham, 2016): 3-23

Makulilo, A. B. "The Future of Data Protection in Africa." In *African Data Privacy Laws*, pp. 371-379. Springer, Cham, 2016.

Ngwafor, E. "Cameroon: The Law across the Bridge: Twenty Years (1972-1992) of Confusion." *Revue générale de droit* 26, no. 1 (1995): 69-77.

Nwocha, M. E. "Customary law, social development and administration of justice in Nigeria." *Beijing L. Rev.* 7 (2016): 430

Olinger, H.N., Britz, J.J & Oliver, M. S. "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa." *The International Information & Library Review 39.1* (2007)

Pasquale, F. *The black box society: The Secret Algorithms that control Money and Information.* Harvard University Press, 2015.

Purtova, N. "The law of everything. Broad concept of personal data and future of EU data protection law." *Law, Innovation and Technology* 10, no. 1, (2018) 40-81

Rich, C. "Privacy laws in Africa and the Middle East." *The Bureau of National Affairs, editor. Privacy and Security law report*. Bloomberg: BNA, (2014).

Robinson, N., Graux, H., Botterman, M., Valeri, L. "Review of the European Data Protection Directive." (Rand Europe, 2009). xiii. Available at https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf Accessed 3/2/2019

Rouvroy, A. & Poullet, Y. "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy." In *Reinventing data protection?* pp. 45-76. Springer, Dordrecht, 2009.

Schwartz, P.M. & Solove, D. J. "Reconciling personal information in the United States and European Union." *Cal. L. Rev.* 102 (2014). 877

Solove, D. "The New Vulnerability: Data security and personal information." In Chander, A., Gelman, L., & Radin, M. J. (2008). *Securing privacy in the Internet age*. Stanford University Press. (2008).112

Solove D. & Citron, D. K. "Risk and Anxiety: A Theory of Data-Breach Harms." *Tex. L. Rev.* 96: (2017) 737.

Ubena, J. "Tanzania lag on privacy law." *Tanzania Legal News*, published online on 8th June 2010, https://tanlex.wordpress.com/2010/06/08/tanzania-lag-on-privacy-law/ Accessed 28 October 2019

Wabwile M. N. "The Place of English Law in Kenya." *Oxford University Commonwealth Law Journal* 3, no. 1 (2003): 51-80.

Wachter, S. & Mittelstadt, B. "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI." *Colum. Bus. L. Rev.* (2019). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Accessed 15/03/2020.

Westin, A. *Privacy and Freedom*. Atheneum: New York, 1967

## Chapter 4: Examination scripts as personal data: The right of access as a regulatory tool against teacher-student abuses in Cameroon universities

Published in *Data Protection and Privacy: Data Protection and Democracy*. Bloomsbury Publishing, 2020.

**Abstract**

Global legal trends are increasingly focused on giving individuals some level of protection of their information, especially information about their personal lives held in online servers of public and private institutions. These trends are particularly concentrated in Europe, and reflected in the Data Protection Directive (DPD) of 1995 and its 2016 successor the General Data Protection Regulation (GDPR), and the 2014 African Union (AU) Convention on Cybersecurity and Data Protection. A right of access to personal data to verify and rectify their accuracy, among other rights, is guaranteed to individuals under these international instruments. With personal data comprising evaluated examination scripts as illustrated in the *Nowak* case, this right of access consequently involves the right to access, verify and rectify the accuracy of an examiner's evaluations on examination scripts.

In this light, this paper advocates that an EU approach to interpreting the AU Data Protection Convention and granting personal data protection rights on examination scripts could yield positive regulatory impacts on African countries in general and Cameroon in particular, in terms of tackling professor-student abuses in university campuses. Granting Cameroonian citizens (and thus university students) an EU-interpreted data protection right to access and rectify the accuracy of their personal data (evaluated examination scripts) could provoke transparency and accountability, and consequently encourage more responsible behaviour from power-abusing staff in institutions of higher learning in the country.

**Keywords**: Examination scripts, right of access, teacher-student abuse, African Union, Cameroon

## 4.1 Introduction

Access to information, considered a basic human right, is guaranteed in a number of international instruments[267], and is a primordial factor of economic development and democratic governance especially in view of meeting up with the challenges of an information society, and has always occupied top positions in development agendas for developing countries.[268] However, while the literature and development programs in most developing countries focuses much more on promoting access to and verification of public information through measures like open data initiatives[269], not so much effort has or is being directed towards access to and verifying the accuracy of personal information. Taking cue from the European approach to personal data protection law, specifically its material scope under the Data Protection Directive (DPD) and its successor the General Data Protection Regulation (GDPR)[270], this paper generally intends to show that the right to access and rectification of personal data processed by public or private institutions could be a source of empowerment and could provoke consequential auto-regulation within certain sectors with specific regulatory needs. In particular, the paper argues that an interpretation of the notion of personal data under the African Union Convention on Cybersecurity and Data Protection similar to the EU approach to personal data protection, coupled with a corresponding right of access to personal data, could help curb teacher-student abuses in institutions of higher learning in Cameroon.

Such interpretation is not so far-fetched: while the AU Data Protection Convention adopts an identical, almost word-for-word definition of personal data as the DPD and GDPR, and also incorporates a right of access to personal data, Cameroon legal practitioners, like in many other former European colonies, in some areas of law, still rely on European (that is, English and French) case law and instruments to render justice in national courts. And the EU notion of personal data protection law appears to be an extension of the EU legislator's objective to provide individuals with a high standard of protection as regards their online information, including vesting in them the widest possible rights

[267] Article 9 of the African Charter on Human and Peoples' Rights, Article 19 of the Universal Declaration of Human Rights, Article 10 of the European Convention on Human Rights, Article 19 of International Covenant on Civil and Political Rights.

[268] See for example Section 72(b) of the African Union's Agenda 2063, published April 2015. Also see the United Nations Economic Commission for Africa (UNECA). "*Harnessing ICT, Science and Technology for Development in Africa*" UNECA Report. November 2007

[269] See for example the United Nations Development Program, "The Africa Data Revolution Report", May 2016. Also see generally Manyika et al. "Big data: The next frontier for innovation, competition, and productivity." McKinsey Global Institute (2011).

[270] 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.

to control and decide what happens to their data after it is collected from them, who has access to its exploitation, to whom it is transferred, even who as much as sees it. These rights, as shall be discussed later, also include access to their data at any time, to verify that they accurate and up to date.

The intention by the EU legislator to offer a high standard of protection to individuals as regards information they share about their online lives has led the former to adopt a very broad interpretation of what constitutes 'personal data'. Some authors think this already broad interpretation is bound to expand even further as we increasingly approach what has been referred to as an onlife[271] experience, where our daily existence is mediated by information technology, and everything around us– weather, waste water, transportation– is being increasingly 'datified', and literally any data can be plausibly argued to be personal.[272] Despite criticism by some authors that the concept of personal data is getting too broad because current available technology can be used to trace just about any information back to an identified individual[273], the fact remains that this approach is leading to the development of new rights which were hardly addressed before, or may been difficult to enforce under other branches of law. This is particularly evidenced in the judgment of the European Court of Justice (ECJ) in the case of *Peter Nowak v Data Protection Commissioner*[274] where the court ruled that the examiner's notes on an evaluated examination script consisted the examination candidate's personal data within the context of European data protection law. One would imagine that prior to this decision or the emergence of data protection law, the legal regime bearing on determining whether or not examination candidates can request to view their evaluated examination script was limited solely to their contract with the examining institution, or to specific sectoral rules regulating the higher education sector. Now EU case law has established such access to personal data (operating alongside the right to personal data protection) as constituting a fundamental right for every EU resident, which automatically enables enforcement, by a student, of the right to verify his/her script and confirm the accuracy of the examiner's corrections. Also worth noting is the fact that the development of European data protection law, though currently a fundamental right on its own[275], was prompted as a result of the limitations of

---

[271] The 'onlife' coined by Luciano Floridi to denote 'the new experience of a hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline' (Luciano Floridi, 'Introduction' in Luciano Floridi (ed), The Online Manifesto. Being Human in a Hyperconnected Era (Springer, 2015), 1).

[272] Nadezhda Purtova. "The law of everything. Broad concept of personal data and future of EU data protection law." *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.41

[273] See Paul Ohm. "Broken promises of privacy: Responding to the surprising failure of anonymization." *Ucla L. Rev.* 57 (2009): 1701-1777. 1756 – 1758. Also see Paul Schwartz and Daniel Solove. "The PII problem: Privacy and a new concept of personally identifiable information.""NYUL rev. 86 (2011): 1814. 1877.

[274] Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994

[275] Article 8 of the Charter of Fundamental Rights of the European Union of 7th December 2000 expressly provides for the right to "The Protection of personal data". This right was further reiterated in Article 16 of the Lisbon Treaty

the right to privacy guaranteed under Article 8 of the 1950 Convention on Human Rights in the wake of new developments especially in the area of information technology[276]. But this broad interpretation, in terms of protecting individuals, appears to extend the material scope of EU law back in time, to protect elements which existed before the digital era, are not affected by technology and yet at that time appeared to be out of the reach of the right to privacy.

The ECJ decision in the *Nowak* case, with regard to the education sector in developing countries, could be groundbreaking from an educational point of view, as it introduces a new dimension to the rights which an examination candidate or student may have vis-à-vis their examining institution or university respectively. This could not only empower examination candidates and students in public and private institutions of higher learning, but could also automatically oblige these institutions and their staff, as data controllers and processors, to adopt more responsible behaviour vis-à-vis their students. Such an approach, if followed by African judges in their interpretation of the AU Data Protection Convention, could play a significant role in regulating teacher-student abuses in universities of developing countries, which include sexual favours for grades, 'sorting' or failing students for non-academic or personal reasons. It is in this light that this paper investigates the potential regulatory role which an EU-based interpretation of the AU Data Protection Convention's right of access to personal data could play in limiting teacher-student abuses on Cameroon university campuses. With no comprehensive legislation in the country specifically governing personal data processing, no related caselaw yet and the AU Data Protection Convention not yet in effect, this paper aims to demonstrate that offering and enforcing EU-inspired data protection rights of access to students in Cameroon vis-à-vis their evaluated examination scripts as personal data could be a major incentive in promoting desired conduct from potentially offending professors and lecturers. In doing so, it also engages the argument that personal data protection law, in particular the right of access, could complement government effort and other areas of law where these may be inadequate in dealing with teacher-student abuses in a third world setting.

The paper shall, in the following chapter, identify some instances of teacher-student abuse in Cameroon universities and discuss the current national efforts and related inadequacies in addressing the issue. The third chapter shall feature a brief synopsis of the notion of personal data in EU data protection law, a discussion on the right of access to personal data under EU law and an overview of

signed on 13th December 2007, which entered into force on 1st December 2009. See also Orla Lynskey. *The foundations of EU data protection law*. Oxford University Press, 2015. pp 91-93

[276] Paul de Hert, and Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Reinventing data protection*?, pp. 3-44. Springer, Dordrecht, 2009. pp 5-6

the *Nowak* case, while the fourth chapter shall focus on the concept of personal data and right to access to evaluated examination scripts as personal data under the AU Data Protection Convention. The fifth chapter shall first examine the state of the art of the right of access to evaluated examination scripts in Cameroon universities before discussing the regulatory effects which a potential EU-inspired interpretation of the notion of personal data and right to access under the AU Data Protection Convention could have in deterring teacher-student abuses in institutions of higher learning in Cameroon. It equally identifies and discusses a few hindrances which could be encountered in the practical enforcement of a right of access on university professors and staff. A sixth and final chapter shall then present the final conclusions.

## 4.2 Teacher-Student Abuses in Cameroon Universities: An Overview

This Chapter examines the phenomenon of teacher-student abuses in Cameroon universities. It shall briefly identify some known examples of teacher-student abuses which affect the sector, before discussing available (though limited) means of protection for affected students.

### 4.2.1 Some Forms of Teacher-Student Abuse in Cameroon Universities

Here, the paper will identify some of the teacher-student mistreatments which plague universities and other institutions of higher learning in Cameroon. The abuses identified here are not exhaustive, and in view of the objective of this paper, are selected on the basis of how the enforcement of a right of access to personal data could significantly reduce their prospective occurrences and incentivise more responsible behaviour on the part of unruly professors or lecturers.

#### 4.2.1.1 Sexual Abuse for Grades

Sexual abuse for grades in institutions of higher learning is not peculiar to Cameroon alone[277]; it is also a systematic occurrence in other African states[278]. Within a lecturer-student relationship, it is not uncommon for some lecturers to demand sexual favours from students in exchange for better grades, whether or not these grades are properly deserved.[279] Cameroon universities do play host to this phenomenon, but as these forms of sexual violence are not often reported[280], data for quality research

[277] For a general overview of the state of sexual abuse in Cameroon, see Mbassa D. Menick. "Sexual abuse at schools in Cameroon: results of a survey-action program in Yaounde." *Médecine tropicale: Revue du Corps de Santé colonial* 62, no. 1 (2002): 58-62.

[278] See generally Louise Morley. "Sex, grades and power: gender violence in African higher education." In *CHEER Symposium, Annual SRHE Conference*, 14-16 December, Newport, Wales. (2009).

[279] See Bukola Adebayo and Stephanie Busari "Lecturer demanded sex in return for better grades, Nigerian student says", CNN news article, published online on May 23, 2018. Retrieved from https://edition.cnn.com/2018/05/23/africa/sex-for-grades-university-nigeria-intl/index.html Accessed 23/09/2018

[280] See Francis Ajumane. "Cameroon: female journalists rise up against sexual assault" Published online on 15/08/2018. Retrieved from https://www.journalducameroun.com/en/cameroon-female-journalist-rise-sexual-harassment/ Accessed 25/9/2018

on the issue is rare. But the incidents are not: a guidance counselor for the Faculty of Social and Management Sciences of the University of Buea, in a 2012 interview, stated that a majority of female students have experienced one or two forms of sexual abuse from male academic staff on campus. These assaults often happen in the office and in lecture halls, when students are requesting make-up tests or extra lectures, submission of overdue assignments, and making other pleas to male academic staff.[281] In her 2011 article on sexual violence on university campuses, Zoneziwoh notes that research studies on sexual violence in the University of Buea were highly underexplored. Victims preferred to report their sexual victimisation to friends, families, colleagues and peers – instead of seeking formal counseling. She blamed this on the fact that there are no established bodies on campus created specifically to handle cases of sexual violence on university campuses.[282]

#### 4.2.1.2 'Sorting'

'Sorting' refers to the negotiation of examination scores with course instructors and school authorities using incentives.[283] This dimension of examination malpractice is currently gaining grounds in universities of some developed countries, and is one of the practices which academic staff who seek personal enrichment involve themselves in.[284] There is a high manifestation of sorting in examinations in Cameroon universities.[285] In the University of Buea, a study shows that sorting is also initiated by lecturers who compel students to purchase their handouts (photocopies of lecture notes). To ensure that students get these handouts, they take down the names of the students who have paid for them. Students who then have their names on the list are compensated through marks, while those who did not buy the handouts are penalised by poor grades.[286] Because exam scripts are usually marked only by the professor and with virtually no direct oversite and feedback, he/she remains in total control of the grading; thereby making it extremely difficult for affected students to prove (or even be aware) that they had been cheated of their marks.

---

[281] Wondieh M. Zoneziwoh. *Sexual Violence on University Campuses: The Case of University of Buea*. No. 2. ALC Working Paper, 2011.7

[282] Ibid, 6

[283] Peter Tambi Agborbechem. "'Sorting' in examinations: Evaluating the quality of assessment in Universities in Cameroon." *International Research Journal of Arts and Social Science* Vol. 4(5) pp. 093-097, June, 2015. 93

[284] Chris Willott. "Factionalism and Staff Success in a Nigerian University: A Departmental Case Study." *States at Work: Dynamics of African Bureaucracies* (2014): 91-112. 95

[285] Peter Tambi. "'Sorting' in examinations" 2015. Ibid. 97

[286] Ibid. 95

#### 4.2.1.3 Failing Students for Personal Reasons

There has been considerable literature on the unequal power relations between professors and students in institutions of higher learning[287]. Within the educational context, there often is a struggle between asymmetrically positioned individuals [professors and students, in this case], which renders one individual as powerful and the other as powerless[288]. The teacher-student relationship has also been described in terms of a transactional process, whereby teachers are in control of curriculum links and teaching styles, and students are oppressed receivers of selected information[289].

This power imbalance is quite glaring in institutions of higher learning in Cameroon, where the lecturer or professor dictates the rules of his/her course and reigns supreme thereon. Due to this somewhat unrivaled status, some professors sometimes tend to abuse their power, even, and not unusually, for selfish or personal reasons. In Cameroon universities, as well as in other African universities, reports about lecturers giving undeserved grades to students because of personal disagreements, off-campus rivalries or for other purely non-academic reasons are not totally unheard of.[290]

The above state of affairs generally favours the victimisation of students by unruly university members of staff, contributing to the bulk of educational troubles in the country. There have been attempts by the state towards establishing a legal framework to sanction abusive lecturers, but these are currently inadequate and reflect a lack of vehemence in state action to address the issue.

### 4.2.2 Regulating Teacher-student Abuse in Cameroon: Inadequacies in National Efforts

Rather unfortunately, very little has been done so far by government agencies and lawmakers in Cameroon to directly and actively address teacher-student abuses in the country. Action so far has been limited to the adoption of legal texts bearing generally on education in the country which provide general protection for students on school campuses and, to a lesser extent, general criminal law.

#### 4.2.2.1 Higher Education Regulatory Texts

For higher education i.e. universities, Law No.005 of 16 April 2001 prohibits 'any violation of human dignity' in state and private institutions of higher learning[291], while Law No.98/04 of 14th April 1998

---

[287] For a general literature review on power relations between teacher and student, see Sharnae Ladkin. "Exploring Unequal Power Relations within Schools: The Authenticity of the Student Voice." *Journal of Initial Teacher Inquiry* 3 (2017): 37.

[288] Sharnae Ladkin. "Exploring Unequal Power Relations within Schools". Ibid. 38

[289] ibid

[290] This phenomenon also occurs in Western societies. See for example Kaitlyn Schallhorn. "Professor fails student for refusing to condemn her Christian faith." Published 5/5/2015. Retrieved from https://www.campusreform.org/?ID=6490 Accessed 26/9/2018

[291] Article 29(3) of Law No. 005 of 16 April 2001 laying down Guidelines for Higher Education in Cameroon

guarantees the physical integrity of the secondary school student, and prohibits 'any form of abuse' on secondary school campuses.[292] There is currently no national law or decree which clearly defines and directly addresses teacher-student abuse with clearly laid down enforcement mechanisms against the phenomenon, and most university student guidelines and administrative texts in the country are practically silent as regards available means of redress which students may have against abusive members of staff or university authorities.

Admittedly, however, Decree 93/035 of 19th January 1993 on the Special Status of Higher Education Staff contains some provisions in this direction. Article 48 of the Decree sparsely mentions the obligation by university professors and staff to ensure the smooth functioning of the teaching activity and safeguard academic dignity. The Decree does not specifically address teacher-student abuse, though Article 51 provides for unspecified disciplinary sanctions on university staff for, inter alia, 'violations of the general rules listed in Article 48', for 'professional misconduct' and for 'participating in any activity incompatible with academic dignity and ethics.' The Decree also provides for the creation of a Disciplinary Council in each state university with the powers to sanction generally unruly personnel[293]. Though it is not expressly mentioned that this Council can entertain cases of student abuse, it can be inferred by analogy that an abused student can, in theory, report their dilemma to the university Rector who, as per Article 55, has the power to seize the Disciplinary Council and summon the concerned lecturer for a hearing, which takes place *in camera*.[294] However, in cases of abuse involving examination scripts, as shall be discussed later, the lack of a right of access to evaluated examination scripts prevents students from being absolutely certain they have been discriminated against. They would generally therefore prefer silence than risk having a Disciplinary Council seized for an unfounded claim.

#### 4.2.2.2 National Criminal Law

Situations of student-teacher abuse, being purely educational issues, are generally less likely to fall within the ambit of criminal law. However, criminal law could be triggered when it comes to student abuse of a sexual nature. Cameroon criminal law punishes the use of one's position of power to obtain sexual favours from a vulnerable individual,[295] a provision which can be invoked by students who face similar situations with a professor. But in a Cameroon university setting, as has been mentioned above,

[292] Article 35 of Law No.98/04 of 14th April 1998 laying down Guidelines for Education in Cameroon.
[293] Article 54
[294] Article 56
[295] Article 302, Law No. 2016/007 of 12th July 2016 establishing the Cameroon Penal Code

these cases are hardly reported[296] not only because they are difficult to prove, but also because of the dominant psychological position professors enjoy vis-à-vis their students. Also, criminal law requires inquiries, investigations, interviews and convocations which may lead to unwanted publicity. And in a third world country like Cameroon, such processes are almost always plagued by bureaucracy bottlenecks, are very slow or lack the input of qualified staff and trained judicial investigators to carry them out efficiently[297].

#### 4.2.2.3 Absence of an Official Code of Ethics for University Professors

Unlike other sectors of activity like the medical and legal professions in the country, the higher education sector of Cameroon is yet to adopt an official code of ethics for university professors and lecturers. The rules in force closest to regulating this sector of activity in terms of professional conduct are those cited above in the Decree of 19th January 1993 sanctioning general misconduct by university staff. Though acts of abuse like sexual harassment or grading discrimination are normally generally frowned at in university settings, the lack of an official code of conduct guiding the higher learning profession only reflects the current apathy of the government and its competent agencies in vehemently addressing teacher-student abuse in university campuses in the country. Nonetheless, this state of affairs could change soon: the Ministry of Higher Education officially launched discussions on 30th May 2019 towards the elaboration of an official code of ethics for university professors and staff members in the country[298].

This Chapter identified some instances of teacher-student abuse as well as the current inadequacies in national efforts to seriously address the phenomenon. This paper argues that providing individuals with a right to access and verify the accuracy of their personal data (in this case, evaluated examination scripts to verify the accuracy of the examiner's evaluation) would, besides complementing the current efforts, significantly contribute to checking the prevalence of these malpractices in the country's universities. This right of access, inherently offered and successfully applied under European data protection law as shall be discussed in the next Chapter, is also offered in the main regional text on African data protection law. However, there is yet to be a legal interpretation or caselaw applying this right to examination scripts on Cameroonian or anywhere in Africa. It is the view of this paper that a legal interpretation, in Cameroon and by Cameroon legal

[296] See note 14
[297] See generally Transparency International. *Global Corruption Report 2007: Corruption in Judicial* Systems. Cambridge.
[298] Jeanine Fankam, 'Enseignement supérieur: un code éthique pour les enseignants en gestation.' Published 7th June 2019. Available at https://www.cameroon-tribune.cm/article.html/26118/fr.html/enseignement-superieur-un-code-ethique-pour-les-enseignants-en-gestation. Accessed 20th June 2019.

practitioners, first of what constitutes personal data and subsequently the right of access to personal data as it has been so interpreted and applied in Europe, could help regulate these misconducts and foster responsible behaviour by unruly university staff. The following Chapter, in the first place, briefly examines the notion of personal data and the right of access to personal data (and consequently evaluated examination scripts) as it applies within the European legal system.

## 4.3 Personal Data and the Right of Access in EU Data Protection Law

European data protection law has been hailed as the legal system which currently offers the highest protection for individuals with regard to the processing of their digital personal information by private companies or public institutions.[299]The regional legal regime does not only aim to protect the privacy of online users with regard to how their information is collected and with whom it is shared, but also extends to giving them the a high level of control over how the information is used, and who gets to use it. As described by De Hert et al, while privacy law protects the opacity of the individual by prohibitive measures (non-interference), data protection calls for transparency of the processor of personal data enabling its control by the concerned individuals, states and special authorities. It puts the activity of the processor in the spotlight, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor's accountability.[300] In other words, the European legislator has adopted a sort of 'defence by attack' strategy of protection: protecting individuals not only by imposing processing restrictions on the data controller, but also by enabling them to leave the shell of their 'privacy' and oversee the activity of the data controller over their data by providing them with a right of access to (the processing of) their personal data. Or generally, by granting control to individuals over data processing activities which might affect them[301]. In this light, this Chapter shall, in the first place, examine the concept of personal data, before focusing on the right of access (to personal data) under European data protection law.

### 4.3.1 The Concept of Personal Data

Perhaps the most fundamental notion of data protection, personal data determines the material scope of the two main texts of reference of European data protection law, the 1995 Data Protection Directive

[299] Ameesh Divatia. "GDPR and the 'Security By Compliance' Mistake", 22nd July 2018. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/02/gdpr-and-the-security-by-compliance-mistake/#1ca90fb5ecc4 Accessed 29/9/2018

[300] Sjaak Nouwt, *Reinventing data protection?* Edited by Serge Gutwirth, Yves Poullet, Paul de Hert, and Cécile de Terwangne. (Preface) Dordrecht: Springer, 2009.x

[301] Peter Hustinx. 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* (2013): 1-12. 2

(DPD now repealed) and the GDPR[302]. The data protection mechanism is triggered only when personal data is processed (Article 3(1) DPD and Article 2(1) GDPR), hence its major significance.

Under the GDPR, which closely follows the DPD 'personal data' is defined as:

> '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.'[303]

If there is one striking thing about the concept of personal data under European law, it certainly is its very broad scope. In its quest to offer a high standard of protection to information society service users, the EU legislator chose to adopt a definition of personal data which could be stretched, it has been argued, to include virtually every type of information.[304] As noted by the Article 29 Working Party[305], the European Commission's original proposal explained that "as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual", and the Commission's modified proposal noted that "the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual." [306] The EU approach is therefore clear: any information 'concerning' an individual should be treated as personal data, which further makes a case for evaluated examination scripts to consist personal data. In this light, and to further elucidate this point, the terms 'any information' and 'relating to' should be paid close attention to.

#### 4.3.1.1 'Any information'

The term 'any information' contained in the Directive clearly signals the willingness of the legislator to design a broad concept of personal data, and calls for a wide interpretation of the concept.[307] It should be pointed that while explaining the meaning of 'any information' within the meaning of the

[302] It should be pointed out that although the Data Protection Directive has now been repealed by the General Data Protection Regulation, this does not affect the concept of personal data as it was under the Directive. See the Opinion of Advocate General Kokott [3] in Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994

[303] Article 4(1) GDPR.

[304] Nadezhda Purtova. "The law of everything", 49, 66

[305] The former EU advisory authority on the matters of data protection, composed of national data protection authorities and headed by the European Data Protection Supervisor. With the coming into force of the GDPR in May 2018, it was replaced by the European Data Protection Board (EDPB).

[306] Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007 ('WP 136').4

[307] Ibid, 6

1995 Data Protection Directive, the Working Party does not define or elucidate on the concept of information itself, but rather goes on to explain what kinds of information would be considered 'any information' in EU data protection law. This only leaves the definition of information in personal data protection context open to interpretation and tends to further expand the scope of what may constitute personal data, stretching the limits of the material scope of EU data protection law. The Working Party noted that personal data could be information not limited *strictu sensu* to private or family life, but information 'regarding whatever types of activity is undertaken by the individual, like that concerning working…the economic or social behaviour of the individual.'[308] Considering that an evaluated examination script contains data showing an individual's behaviour when confronted with a given set of problems (even hypothetical or imaginary problems), it should still be regarded as personal data in EU data protection law.

Another interesting interpretation advanced by WP136 is that information could be personal data whether processed by non-electronic means[309], and regardless of the format or medium in which the information is contained. It could be numerical or, ideally, information kept on paper.[310] An examiner's written evaluation on an examination script perfectly fits these criteria.

#### 4.3.1.2 'Relating to'

The WP29 referred to this building block of the definition of personal data as 'crucial as it is very important to precisely find out which are the relations/links that matter and how to distinguish them.'[311] It advances, in general terms that information can be considered to "relate" to an individual when it is *about* that individual.[312] In a prior Opinion, in 2005, on data protection issues raised by RFID tags, the WP29 had established that "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated."[313] Seen in this light, evaluating examination scripts serves one main purpose: that of evaluating the student, the result of which will determine his/her future within and out of an institution.

WP29 further establishes that information could "relate to" a person in terms of 'content', 'purpose' or 'result'.[314] The 'content' element is fulfilled when the information is clearly about the

[308] Ibid
[309] Ibid, 5. Also Article 2(1) GDPR
[310]
[311] Ibid, 9.
[312] Ibid.
[313] Ibid, 10.
[314] Ibid

person e.g. medical examination results under a person's name; the 'purpose' element 'can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to *evaluate*, treat in a certain way or influence the status or behaviour of an individual (emphasis added); and as regards the 'result' element, data can be considered to "relate to" an individual because their use is likely to have an impact on a certain his/her rights and interests.[315] This European Court of Justice concurred with this reasoning as regards an examiner's evaluative information on an examination script in the case of *Peter Nowak v. Data Protection Commissioner*[316].

#### 4.3.1.3 Evaluated Examination Scripts as Personal Data in EU Data Protection Law (*Peter Nowak v. Data Protection Commissioner*)

In 2017, a landmark decision was reached in the case of *Peter Nowak v. Data Protection Commissioner,* with regard to data protection law in the education sector. In 2009, Peter Nowak, a registered student with the Institute of Chartered Accountants of Ireland (CAI) asked to view his scripts for an accounting exam after failing it for the fourth time, with a view to challenging the result. The CAI declined releasing the exam script, saying it did not constitute personal data under data protection legislation. Mr Nowak sought assistance from the Data Protection Commissioner, but was rejected on the same grounds as with the CAI. After appealing to the Circuit Court, then the High Court, the case got to the Supreme Court which decided to ask the European Court of Justice for guidance. In its reference for a preliminary ruling, the Irish Supreme Court essentially asked whether the exam script containing the candidate's answers and the examiner's comments regarding those answers might constitute personal data.[317] Both the response by Advocate General of the European Court of Justice (in her Opinion) and the Court were in the affirmative.

The Advocate General's reasoning was consistent with the WP29 approach to consider information as personal data when it is processed with a purpose of evaluating the status or behaviour of an individual. Even though the examination exercises are 'formulated in abstract terms or relate to hypothetical situations',[318] 'the script is a documentary record that that individual has taken part in a given examination and how he performed'[319]. She further states that 'in every case, the aim of an examination […] is to identify and record the performance of a particular individual, ie the

[315] Ibid, 10-11
[316] Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994
[317] Nowak (n 9), Opinion of Advocate General Kokott [2].
[318] Ibid [19]
[319] Ibid [21]

examination candidate. Every examination aims to determine the strictly personal and individual performance of an examination candidate'.[320]

The Court followed the reasoning of the Attorney General. It reaffirmed the notion 'personal data' as potentially encompassing any information, as long as it 'relates' to the data subject[321], stating that the condition is met where the information is linked to a particular person 'by reason of its content, purpose or effect'.[322] Most significant, the Court found that the link between the information and the individual relevant because both the candidate's answers and the examiner's comments relate to the data subject in all three aspects: they reflect the information about the candidate (his knowledge, thought process and, in the case of a handwritten answer, information about his handwriting, as well as the examiner's opinion regarding the candidate's performance)[323]; the purpose of their processing is to evaluate the candidate in terms of his professional abilities; and the use of this information is 'liable to have an effect on his or her interests'[324].

### 4.3.2 Right of Access to (and Rectification of) Evaluated Exam Scripts in EU Data Protection Law

European data protection law has, from the outset, pursued dual objectives. One of these objectives is economic—to facilitate the establishment of the internal market—while the other is rights-based—to protect fundamental rights when personal data is processed.[325] The right of personal data protection as well as a right of access to personal data are well established in the EU Charter of Fundamental Rights (CFR) of 18th December 2000. Captioned 'protection of personal data', Article 8 of the Convention states:

> éé"Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

[320] Ibid [24]
[321] *Nowak* (n 9), [34].
[322] Ibid [35]
[323] Purtova (2018) Ibid, 71
[324] Nowak (note 8), [39]. But see *YS and others* (17th July 2014, ECLI:EU:C:2014:2081) [46] where the ECJ created a precedent to the effect that the right to access a document affecting one's interest is not absolute and may be denied in certain circumstances (in this case, if it will lead to granting access to administrative documents). The Courts usually balance the right of against other fundamental rights and interests, to determine its enforcement. See Antonella Galetta and Paul de Hert. "A European Perspective on Data Protection and the Right of Access." In *The Unaccountable State of Surveillance*, pp. 21-43. Springer, Cham, 2017. p 35.
[325] Orla Lynskey. *The foundations of EU data protection law*. Oxford University Press, 2015.46

This Article not only explicitly mentions a right to data protection, but also explicitly creates a concurrent right of access to personal data, as well as the right to have it rectified, to ensure accuracy. The right of access to personal data is therefore expressly guaranteed as a functional tool of the right to data protection in EU law. The Data Protection Directive states that the principle of data protection should be reflected both in the obligations imposed on data controllers for responsible processing as regards quality and technical security, and also in the right conferred on individuals "to consult the data, to request corrections and even to object to processing in certain circumstances".[326] The right of access under the Article 12 of the Directive is a four-fold: the data subject may ask confirmation as to whether or not his data are being processed; he has the right to obtain communication of these data i.e. have copies of the data being made available to him; he can have the data rectified, erased or blocked if they do not conform to the Directive, in particular if they are incomplete or inaccurate; and the right to be informed about the logic used in case of automated decisions. The right of access to personal data under the 1995 Directive, it can be concluded, incorporates two important components in relation to this paper: the right of data subjects to be presented with their personal data, and their right to have that data rectified.[327]

The GDPR closely follows this approach, recommending that a data subject should have "the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing."[328] However, and moving slightly away from the approach of the CFR, it provides for the right of access (Article 15) and the right of rectification (Article 16) in two separate Articles, which suggests that these rights are two separate rights under the GDPR. Nevertheless, the enforcement of a right of access, in event of established data inaccuracy, will most likely involve the right to rectification by ricochet. In other words, the former is necessary for the realisation of the latter[329]. It follows that if examination scripts are personal data under European law, then a student is apparently well within his/her data protection rights if they request access to their evaluated examination script being processed by an examining institution in order to verify the accuracy of the evaluation, and demand its rectification if need be.

---

[326] Recital 25, Data Protection Directive

[327] Antonella Galetta and Paul de Hert. "A European Perspective on Data Protection and the Right of Access." Ibid. p 25. Also see generally Raphael Gellert and Serge Gutwirth. "The legal construction of privacy and data protection." *Computer Law & Security Review* 29, no. 5 (2013): 522-530.

[328] Recital 63, GDPR

[329] *YS and Others* ibid, Note 58 [44]

This was apparently the view of AG Kokott in the *Nowak* case. In response to the question as to whether the examination candidate had a right to access his data, her opinion was in the affirmative, stating that he 'has a legitimate interest, based on the protection of his private life' to be able to object to the processing of his or her examination script outside the examination procedure.[330] The ECJ upheld this view[331], ruling further that the rights of access and rectification provided for in Article 12(a) and (b) of the Directive "may also be asserted in relation to the written answers submitted by a candidate at a professional examination and to any comments made by an examiner with respect to those answers."[332] The above show that EU data protection law does not only qualify examination scripts as personal data, but also guarantees a right of access to verify that these scripts have been fairly evaluated. As was seen in *Nowak,* this enabled the examination candidate (plaintiff) to at least see how his script was evaluated and, if he so desired, demand that the grades be made accurate if they are inaccurate within the meaning of Article 6(1)(d) of the 1995 Directive.

It should be noted however that the right of access to (and rectification of) personal data is not an absolute right, and may be limited in some instances in EU law.[333] As a matter of fact, it has been rejected by the ECJ in a case which, if granted, would have laid a precedence for access to administrative documents of a country's immigration office[334]. Wachter & Mittelstadt are also of the opinion that the ECJ does not intend to use data protection law as a tool to ensure accuracy or total transparency in decision-making processes involving personal data, leaving that to specific sectoral laws.[335] However, as noted by the Article 29 Working Party, data protection law envisages the possibility of personal data being incorrect, and provides for a right for data subjects to access their personal data in order to rectify it.[336] And a careful analysis of the ECJ's interpretation of inaccuracy of examination results in *Nowak* within the meaning of Article 6(1)(d) would lead to the understanding that an examiner's unfair comments which do not reflect the answers on the script could be regarded as inaccurate data[337], especially considering the premise that the candidate's answers themselves, with or without any grades, are personal data, because they *relate to* the candidate's intellectual level[338].

---

[330] *Nowak* (n 9), Opinion of Advocate General Kokott [26]
[331] *Nowak* (n 9), [50].
[332] *Nowak* (n 9), [51].
[333] See Article 23 of the GDPR, which lists the preservation of 'general public interest' and, slightly relevant to *YS and Others*, independence of judicial proceedings among the reasons for which the right of access may be restricted.
[334] *YS and Others,* Ibid
[335] Sandra Wachter and B. D. Mittelstadt. 'A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI.' *Columbia Business Law Review* (2018).4.
[336] WP136 (n 36) 6.
[337] *Nowak* (n 9), [54].
[338] *Nowak* (n 9), [51].

And if processing (checking the correctness, hence evaluation, and which itself is supposed to be fair, reflecting the data protection principle of fair processing[339]) carried out on this set of personal data yields inaccurate results which will impact a data subject's career, then right to rectification and prior right of access are likely to (or should) be triggered. It should nevertheless be pointed out here that the essence of this paper is not to present data protection and particularly the right of access and rectification as a silver bullet solution for ensuring fair grading of examination answers. Rather, these rights are presented as a tool for reducing the power imbalance between students and professors by making it possible for a graded script to be accessed and even made public (by the candidate) for everyone to see and have an opinion; which could discourage unfair grading by abusive professors as a means to force students do their bidding.

Across the Mediterranean, the AU Convention on Cybersecurity and Data Protection adopts definitions and rights attached to personal data inspired by, and strikingly similar to those of the EU. It therefore is not too far-fetched for African judges and lawyers to interpret these notions and rights similarly to their interpretation by the ECJ. The following chapter presents a brief synopsis of the AU Convention, as well as its adopted notion of personal data.

### 4.4 Personal Data under the AU Data Protection Convention

This chapter shall be an overview of the AU Data Protection Convention, which is inspired from Europe's DPD model. It shall first of all present a brief background of the Convention before examining the similarities between its notion of personal data and that of the DPD and GDPR. After which it shall feature a discussion on its right of access to personal data and, by interpretation, to evaluated examination scripts.

#### 4.4.1 The African Union Convention on Cybersecurity and Personal Data Protection

The AU was established in 2001 to replace the Organization of African Unity, and has its headquarters in Addis Ababa, Ethiopia. Its aims include, inter alia, to 'accelerate the political and socio-economic integration' of the African continent and to "coordinate and harmonize the policies between the existing and future regional economic communities for the gradual attainment of the objectives of the Union'[340] These mandates create a broad legal basis for the AU to establish regional policy and regulatory regimes on issues that affect Africa's economic integration and development, such as telecommunications/ICTs and personal data protection. From 2008, a series of high profile meetings were held between ICT policy makers and economic stakeholders of AU Member States, culminating

[339] Article 5(1)(a) GDPR, Article 13, AU Data Data Protection Convention
[340] Article 3, Constitutive Act of the African Union

in the adoption, by AU Member State ministers in charge of ICTs, of a set of declarations known as the Oliver Tambo Declaration on 5th November 2009 in Johannesburg, South Africa.[341] The Declaration directed the AU to 'jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection.'[342] Five years later, at the 23rd Ordinary Session of the Assembly of Heads of State of the African Union in Malabo on 27 June 2014, the Convention on Cyber Security and Personal Data Protection (hereinafter the AU Data Protection Convention) was adopted.

The Convention provides a legal framework regulating three distinct domains and divided in as many corresponding sections: Electronic Commerce, Data Protection and Cybercrime/cybersecurity. It has as objective, as regards personal data protection, the establishment of 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.'[343] It should be pointed out that unlike the EU, legal integration within the AU is hardly a reality;[344] the Union has been likened to an interstate organisation (with focus on the nation state and regarding regionalism simply as an arena for international politics) rather than a supranational organisation, hence the inability to adopt enforceable decisions which prevents the establishment of a regional legal system through institutional action.[345] As a result, Conventions adopted by the General Assembly of the African Union, when they become effective, are not directly binding on Member States. Only a further Act by a Member States incorporating a Convention into its national legislation renders the Convention applicable in the said state.

The AU Data Protection Convention in question, as of the time of writing this paper, is not yet effective, and will attain this status only upon ratification by 15 member states.[346] Once this quorum is attained, the Convention will serve more like a model law for national data protection purposes. It should be pointed out that the provisions of the Convention are not very detailed, provoking an

[341] Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (2009) *Oliver Tambo Declaration.* Johannesburg, South Africa: African Union.
[342] Ibid, p.4
[343] Article 8(1), African Union Convention on Cyber Security and Personal Data Protection
[344] 'Legal integration' is significantly missing from the objectives of the AU enlisted under Article 3 of the Constitutive Act
[345]Michèle E. Olivier, "The role of African Union law in integrating Africa." *South African Journal of International Affairs* 22, no. 4 (2015): 513-533.p.514
[346] Article 38, ibid

interpretation that they serve rather as a basis for national data protection in legislation in African countries, but nevertheless requiring only a modest amount of detail to be added[347]. So far (June 2019), only fourteen Member States have signed the Convention, among whom only four (Senegal, Namibia, Guinea and Mauritius) have ratified it.

### 4.4.2 Evaluated Exam Scripts as Personal Data: A Prospective AU Interpretation

In delimiting its material scope, the AU Data Protection Convention defines personal data, as follows:

> 'Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by African Union Legal Instrument reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity'.[348]

The closeness to the definition of the notion of personal data by the European DPD and GDPR is quite obvious in these definitions, with the terms 'any information' and 'relating to', appearing in all three definitions. As has already been discussed in the preceding section of this paper, these terms allow for a very broad range of data to fall under data protection law, and data determined to be personal data automatically requires protection and processing restrictions in accordance with the said legal framework. And considering that so far there have been no official guidelines produced by the AU or case law from any intergovernmental African court providing a detailed, succinct, legal and African interpretation of the above definitions of personal data, it seems fairly logical that in applying (and hence interpreting) the above instruments in African courts, reference shall still be made to European legal opinions and case law to reach a decision as regards what should or should not constitute personal data. It therefore can be comfortably concluded that evaluated examination scripts, as was decided in *Nowak*, will most likely be equally interpreted as personal data in an African court.

This tendency of African legislators to follow and apply existing European approaches to solve legal disputes is not at all new. Makulilo has advanced two reasons for this trend in relation to data protection law: first, major legal systems in Africa namely common and civil law legal systems which are Western in origin, create fertile grounds for adaptability of European law. Though these systems were forcibly imposed on Africa by European countries during colonial rule as part of the colonial superstructure and an instrument of coercing Africans to participate in the colonial economy, they

[347] Graham Greenleaf and Marie Georges, "The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?" 131 *Privacy Laws & Business International Report* (2014). 18-21
[348] Article 1 Para.36, African Union Data Protection Convention.

were inherited by African countries upon independence. African countries, arguably, are therefore no strangers to the adaptation of 'foreign law'.[349] The second reason is economic motivation: Makulilo purports that African data protection legislations are modelled upon the EU Data Protection Directive following the desire of African countries to meet the 'adequacy' standard of the European law in order to attract foreign investments[350], a consequence of the so-called "Brussels Effect".[351] Europe represents the world's largest community of consumers[352], and is accompanied by powerful regulatory institutions capable of directly imposing decisions and sanctions on member states, making it one solid, lucrative economic bloc. Given its economic weight, it remains a very attractive market for any ambitious business operator anywhere, rendering its regulations the benchmark to comply with even at global level.

It should also be pointed out that eventuality of an EU-interpretation, of personal data to include evaluated examination scripts as personal data on Cameroon soil is not very unlikely, if not certain. Not only are African countries (slowly but surely) adopting data protection laws[353] inspired by related EU legislations, Cameroon, like most formerly colonised African countries, is by no means a stranger to European statutory or case law. The country is actually bijurial, with the common law and civil law operating simultaneously on the territory, inherited from pre-independence British and French administration. To date, based on Sections 11 and 15 of the 1955 Southern Cameroons High Court Law, common law courts in the English-speaking regions of the country still rely on British jurisdiction and caselaw in litigations on matrimony, probate, tort and contracts between individuals[354], while the French-oriented civil law courts still rely on legal reasoning from French judicial courts in rendering judgments in a range of civil litigations, especially on aspects not yet addressed by national law. Cameroon legal grounds therefore appear fertile enough for the adaptation of EU-inspired interpretation of data protection law within its national territory. This further favours the likely interpretation, upon an incorporation of the AU Data Protection Convention into the

[349] Alex B. Makulilo, 'One size fits all: Does Europe impose its data protection regime on Africa?', *Datenschutz und Datensicherheit-DuD* 37.7, (2013) 447-451.451

[350] Article 25 of the DPD and now Article 45 of the GDPR restrict data transfers of EU residents to countries which do not have an 'adequate' standard of personal data protection. Also see Makulilo, Ibid, 450.

[351] Term coined in 2012 by Professor Anu Bradford to denote the soft power which EU regulations have worldwide, due to the size of its consumer base and strength of its regulatory institutions.

[352] Anu Bradford. "The Brussels effect." *Nw. UL Rev.* 107 (2012): 1.11

[353] By 2015, 17 African countries had adopted comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara. See Cynthia Rich, "Privacy laws in Africa and the Middle East." *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA* (2014).1

[354] Ephraim Ngwafor. "Cameroon: The Law Across the Bridge: Twenty Years (1972-1992) of Confusion." *Revue générale de droit* 26, no. 1 (1995): 69-77. 71

country's national law, of evaluated examination scripts as personal data in Cameroon, including a corresponding right of access and verification.

### 4.4.3 Right of Access to Evaluated Exam Scripts as Personal Data under the AU Data Protection Convention

The AU Data Protection Convention also grants a right of access to individuals whose personal data are undergoing processing in the possession of the data controller. Without expressly using the term "access", it states:

> 'Any natural person whose personal data are to be processed may request from the controller, in the form of questions, the following:
>
> a) Such information as would enable him/her to evaluate and object to the processing…'[355]

Paragraph (a), by obliging the data controller to provide the data subject with information which will enable him/her evaluate and object to the processing, creates an implied right of direct access to the processing, especially considering that the term 'information' is not defined under the Convention, and could include anything: from meaningless data[356] to a tangible, evaluated information script. Also, the phrase 'such information as would' and not 'such information about' widens the scope of what the data subject can actually request from the data controller, as information 'about' a data source could be made available to an individual without making available the data source itself. So under this provision, the data subject is not constrained to ask only for information about how his/her data is being processed, but can also ask to be provided with the data source itself, in so far as his/her evaluation and possible objection to the processing can be effectively done only by (directly) examining the data source. Just as in the DPD and GDPR therefore, there also is a right of access to personal data and hence evaluated examination scripts guaranteed under mainstream international African data protection law. The AU Convention also provides for a right of rectification in Article 17, which could be very useful in terms of requesting the re-evaluation of a marked examination script.

Worthy of note is the fact that unlike the DPD and GDPR, the AU Convention does not specify any limits to the right of access to processed personal information. With the Convention not yet in force and, to the best of the author's knowledge, the absence of case law or published African DPA decisions on the right of access to personal data, it is not clear to which exceptions they may be subject to in practice. Nevertheless, considering the relatively low level of privacy awareness in

[355] Article 17, AU Data Protection Convention
[356] See Nahdeza Purtrova (ibid) 52

Africa[357](which, interestingly, is not even listed in the catalogue of rights of the African Charter on Human and People's Rights of 1981), it can be expected that the right will be trimmed with a significant amount of restrictions in its practical enforcement. Current lack of case law in African courts on the subject, however, prevents the formulation of an informed decision on the issue in this paper.

### 4.4.4 Right of Access to Personal Data under the AU Data Protection Convention: Enforcement Mechanisms

Compared to Europe, data protection is pretty new in Africa, with the first concrete steps taken jointly by African ICT ministers to protect online information privacy across the continent being in 2009[358]. This novelty is also reflected in its enforcement mechanisms, with the Data Protection Authority (DPA) appearing to be the sole entity with powers to ensure compliance with data protection rules; it is responsible for "entertaining claims, petitions and complaints regarding the processing of personal data and informing the authors of the results thereto".[359] Interestingly (and rather unfortunately), the AU Data Protection convention does not provide for direct action against data controllers in the courts by individuals who feel their data protection rights have been violated, neither does it specifically create a liability relationship between the data controller and data subjects. This suggestively leaves all forms of redress to be addressed solely to the DPA, who is prescribed to be an independent national data protection authority with immunity from lawsuits (Art.11). The DPA is attributed broad powers in terms of data protection enforcement, including to investigate, issue opinions and warnings, inform judicial authorities of offences, impose monetary fines, or discontinue processing where fundamental rights are threatened (Art.12). The details and limits of these powers appear to be left to the discretion of Member States. The DPA's decisions, however, are subject to appeal before national courts.[360]

This Chapter illustrates that an EU-inspired interpretation of AU data protection law by African legal practitioners would not only lead to evaluated examination scripts being considered personal data on African soil, but would also institute a right of access to these scripts for verification and possible re-correction. This would arguably play a significant role in deterring teacher-student abuses hinged on examination evaluations within the university and higher education in an African and third

[357] See generally Alex Makulilo. 'The context of data privacy in Africa.' In *African Data Privacy Laws*, pp. 3-23. Springer, Cham, 2016.
[358] . In 2-5 November 2009, African Union state ministers in charge of ICTs in their various countries met in Johannesburg and adopted what was referred to as the Oliver Tambo Declaration, in which they urged the African Union Commission to "develop…a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection.
[359] Article 12(2)(e) AU Data Protection Convention
[360] Article 12(6) AU Data Protection Convention

world setting. The following Chapter examines some potential impacts which such a development would have on the fight against this phenomenon in Cameroon, and also identifies and discusses some difficulties which could obstruct the practical enforcement of the right on university staff in the country

## 4.5 Right of Access to Evaluated Exam Scripts as Personal Data in Cameroon: Potential Impacts on Teacher-Student Abuses

One of the objectives of the EU data protection reform of 2012 was 'reinforcing the right to information so that individuals fully understand how their personal data is handled'[361] An objective upheld by the ECJ held in *Nowak,* granting a right of access to information (albeit personal information) to enable an individual appreciate the processing of data which shall have an impact on him. The literature already portrays the right to (public) information as a promotor of transparency and good governance,[362] but so too could be a right to private (personal) information in terms of ensuring control by individuals over the processing of their personal data. Access to data processing implies control over data, empowers the data subject[363] and indirectly imposes a duty of transparency on the data controller, which acts as a regulatory tool. Moreover, such access also gives the data subject the necessary tools to defend himself/herself (in this case, the marked examination script) as required by law in the event of a dispute or criminal proceeding.

This final Chapter shall first of all present a brief review of the current situation of the right of access to examination scripts in Cameroon universities. This shall be followed by a discussion on some potential regulatory effects which could result from an EU-inspired interpretation and application of students' data protection right of access to their examination scripts, as regards deterring teacher-student abuses, and subsequently an examination as to how this right complements current criminal law in combatting this societal ill. This shall be then be followed by a brief identification and discussion of some hindrances which may be encountered in the practical enforcement of a right of access to evaluated examination scripts as a data protection right in Cameroon universities.

### 4.5.1 Right of Access to Evaluated Exam Scripts in Cameroon: A Brief State of the Art

Cameroon is yet to enact and adopt a comprehensive national data protection law, and there currently is no legal mechanism explicitly providing students with a right to access their examination scripts after they have been corrected. The above mentioned Decree No. 93/035 of 19th January 1993 and

[361] 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) 9 final, at 6.

[362] Hielke Hijmans. 'Understanding and Assessing the Contribution of the CJEU to the Mandate Under Article 16 TFEU.' In *The European Union as Guardian of Internet Privacy*, pp. 185-261. Springer, Cham, 2016. 236 et seq

[363] Ibid, 175

Law No.005 of 16 April 2001 are silent on the issue. So too is Decree No. 08/0249/MINESUP of 11th September 2008 on the Common Status of Students in University Institutions of Cameroon. This implies that it is up to the discretion of the universities to determine whether or not to grant such a right to their studentts. The internal rules of the state universities are equally silent on this aspect; the closest to such a right being the right to request for a re-evaluation of the evaluated script in case a students is not satisfied with their grade, and whether or not any re-evaluation shall be done is completely at the discretion of the Faculty Dean. In the University of Yaoundé I, for example, the student has a time limit of up to three days after the official date of publication of the examination results to file such a complaint to the Faculty Dean, and the latter reserves the power whether or not to order for such re-evaluation.[364] Also, the student can request apply to the Faculty Dean for a verification of the total count of marks on his/her script.[365] However, in both cases, the student does not have a right of direct access to the evaluated script.

This is strikingly different to what obtains in Europe, where some universities expressly provide their students with a right of access and verification of their evaluated examination scripts. Leiden University, for example, explicitly grants this right to its Masters students. [366]

### 4.5.2 Right of Access to Evaluated Exam Scripts: Deterring Sexual Abuse for Grades

Despite having ratified most international conventions protecting the women's and children's rights, Cameroon is yet to develop and adopt specific, comprehensive national policies directly addressing sexual abuse in institutions of higher learning in the country. Given such a state of affairs, an EU-interpreted access to personal data in Cameroon could very well be a useful complementary tool to deter sexual abuse. If offering natural persons some level of control over their personal data empowers them with a right of access and verification as illustrated in *Nowak*, then providing students with control over their evaluated examination scripts represents an opportunity to put some checks on the powers of their lecturers or professors. Students who enjoy a right to access their evaluated examination scripts and to verify the accuracy of this evaluation are, as a result, indirectly protected

[364] Article III.2.3 of the Internal Pedagogical Regulations of the University of Yaoundé I of 27th December 2012. Retrieved from http://www.webuy1.uninet.cm/uy1/images/fichiers_attaches/Reglement_Interieur_UY1.pdf Accessed 27th September, 2018

[365] Ibid, Article III.2.6

[366] Article 4.8.1 of the Course and Examination Regulations of the Master's Programme International Relations and Diplomacy, 2018-2019 of Leiden University. Retrieved from https://www.organisatiegids.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/oeren/oeren-juli-2018/oer-m-ird-2018-2019.pdf Accessed 28/9/2018

from being compelled by an unruly university professor or member of staff to perform sexual favours for better grades.

If students have a fundamental right to access their evaluated examination script as personal data in the sense of Article 8 CFR, then they can always expose the unfairness in the grading by a professor who may have done the grading unfairly because the student rejected their sexual demands. This certainly would also auto-regulate related conduct of such professors and discourage them from demanding sexual favours in return for allowing a student pass their course; because being aware that a student can always verify and hence publicly question the professor's grading will certainly be a strong deterrence incentive to deter unfair grading. Granting some personal data control over evaluated examination scripts could therefore contribute significantly in ridding the university milieu of this phenomenon.

### 4.5.3 Right of Access to Evaluated Exam Scripts: Checking the Teacher-Student Power Imbalance

As discussed above, professor-student relations can be viewed as an imbalanced power relationship, with the student being the weaker party. Some professors tend to abuse such powers, which could take the form of failing a student for personal reasons, or if the student refuses to succumb to the 'sorting' antics of a professor, for example failing to buy their handouts. Coupled with the fact that the professor reigns supreme in his course with very little or no supervision from the university administration, victimised students prefer silence than protest.

However, qualification of examination scripts as students' personal data in Cameroon could be a useful tool in balancing the professor-student power equation. As discussed above in *Nowak*, personal data protection guarantees a right of access to evaluated examination scripts. Consequently, as data controller institutions, universities shall suddenly have an obligation towards students to, upon request by the latter, grant them access to their evaluated examination scripts and proceed to process any reasonable rectification claims. Such right to access and rectification, because it exposes and subjects the professor's grading to the scrutiny of the student and that of any other person the student choses to share that data with, manifestly reduces the risk of power abuse by the professor. As similarly concluded in the preceding subsection, knowing that their evaluation can be accessed (and hence questioned before others) at any time by their students would most certainly represent a strong incentive for professors to grade the former accurately and fairly; hence tipping the power balance in the students' favour.

### 4.5.4 Right of Access to Evaluated Exam Scripts: Complementing Criminal Law

As discussed in Chapter 2, Cameroon criminal law offers protection to abused students principally in relation to sexual abuse, with the other identified incidents of teacher-student abuse being more of an educational discipline nature. And even such protection is not easily enforced because most cases go unreported, and the Cameroon criminal process, in practice, faces problems of logistics and trained personnel, similar to most third world countries. In light of this state of affairs, this paper argues that the introduction of a right of access to evaluated examination scripts as personal data could lend a helping hand to criminal law by acting as an *ex ante* a regulatory deterrent with regard to sexual abuse by lecturers on students in a Cameroon university setting.

Considering that unruly lecturers usually use examination grades based on inaccessible evaluated examination scripts as bait to compel students to do their bidding, it appears much easier, instead of depending on criminal law for sanctions *ex post*, to deter such practices simply by rendering evaluated examination scripts accessible to students as a personal data protection right. Thus giving them the opportunity to access and verify the accuracy and fairness of their grades. In other words, instead of relying on criminal procedure which is triggered only after the commission of an offence, a right of access to evaluated examination scripts will serve as a means of keeping potential unruly professors in check; as knowing the student can have access to their script and see first-hand how they have been evaluated (and raise an alarm, if need be) would certainly compel the professor to grade the student fairly. This represents a less rigid and more practical defence mechanism for the students, instead of leaving everything to the bureaucracy of criminal procedure law which will require the issuing of warrants and other cumbersome investigatory processes to uncover evidence of teacher-student abuse.

### 4.5.5 The Right of Access to Evaluated Exam Scripts: Potential Enforcement Hindrances

In as much as a right of access to personal data, as illustrated above, could help regulate teacher-student abuse in Cameroon universities, its practical application may however be faced with some difficulties. The first probable hindrance can be deciphered in the overlapping and possible clash between the university administration as the state-instituted guarantor of the safety and well-being of the student on the one hand, and the national DPA as guarantor of the personal data protection of (Cameroon) citizens on the other. There could be a power struggle between both authorities: with the DPA being empowered by the AU Data Protection Convention to investigate and sanction data controllers, it appears to have the competence to order a professor or concerned/relevant university staff member (who, as regards an evaluated examination script, is the data controller) to produce an evaluated script on the request of the evaluated student. However, professors generally are subject to administrative rules and regulations of their university, and such an order, depending on the

circumstances, could possibly go against university rules or protocol. It therefore could be interesting to see, in the eventuality of the adoption of the Convention and resulting creation of a DPA in Cameroon, how this and similar situation(s) will be managed between both authorities.

Another potential hindrance, closely related to the first, concerns the immunity status of both entities. While the AU Data Protection Convention grants judicial immunity to the DPA (Article 11), Cameroon university campuses also benefit from an inviolability status granted by national law. Article 49 of the Decree of 19th January 1993 for example expressly forbids entry by any law enforcement officer into a university campus to investigate or establish a crime, or to execute any legal order on a university professor or member of staff without a written authorisation of the regional state attorney (*Procureur Général*) presented to the Rector of the concerned university. Similarly, Article 9 of Decree No. 2001/832/PM of 19 September 2001[367] also proclaims the inviolability of private university campuses. While looking forward to a regime of regulatory cooperation between university authorities and the DPA, this state of affairs nevertheless leaves open the possibility of a university invoking its inviolability to block any investigatory mission into its campus by the DPA. Such situations may not be unusual especially where the investigation involves a high-ranking professor of the university, or who weaves significant political influence. Such circumstances could likely hinder the smooth investigation for an access complaint brought by an alleged abused student before the DPA, hence obstructing the practical applicability of a right of access. It is opined in any case that the national legislator shall consider all these circumstances when adopting a national data protection framework guaranteeing a right of access to personal data (including evaluated examination scripts) in the country.

### 4.6 Conclusion

This paper argues that an EU-standard interpretation of the right of access to personal data under the AU Data Protection Convention (when it eventually comes becomes effective) in Cameroon by Cameroonian legal practitioners could contribute positively and significantly to prevent the propagation of teacher-student abuses on university campuses in the country. Professors do wield academic powers over students, which is necessary for the teaching and evaluation process. But when such power is abused, there arises a need to put some checks and balances on it. *Nowak*, though not a case of on-campus abuse, happens to provide a useful tool to attain this need: giving examination candidates a data protection right of access and verification over their evaluated examination scripts.

[367] Decree No. 2001/832/PM of 19 September 2001 to lay down general provisions applicable to Private Institutions of Higher Learning.

As noted by De Hert et al, data protection law tends to provoke the personal data processor into transparency and accountability by giving some level of control over that processing to the individual.[368]If individuals have a possibility of verifying and rectifying their processed data, as they presently do under EU data protection law, then the processors will consequently adopt more responsible behaviour vis-à-vis their personal data.

The same effect could be transposed into Cameroon's higher learning setting, to limit the progression teacher-student abuse. In the likely eventuality that personal data and a related right of access under the AU Data Protection Convention, when it becomes effective, are interpreted in Cameroon by Cameroonian legal practitioners as they are interpreted in Europe, then students could have a right of access and verification of their evaluated examination scripts, just as it was decided in *Nowak*. Which in turn implies that potential unruly professors or lecturers, who usually use unfair grading as the main compelling weapon to force students into accepting their sexual propositions, 'sorting' transgressions or compel other forms of abuse, would suddenly be constrained to grade all students fairly. For a student could then be able to gain access to and verify how their script was graded and, given the parallel data protection right to object to processing, can raise an alarm if he/she feel cheated. Moreover, the country does not currently have any official code of ethics binding university professors and lecturers, which further leaves room for ethical decadence within the higher learning corps. Also, despite abusive conduct like sexual harassment being punishable by the Cameroon Penal Code, such cases are hardly reported for fear of unwanted publicity, or simply because students wish to avoid open confrontations with professors. Coupled with the problem, as in many third world countries, of slow judicial bureaucracy and the lack of qualified, trained judicial staff to effectively investigate such allegations. In light of the above, this paper concludes that that the right of access under the AU Data Protection Convention, if interpreted as in *Nowak*, would provide another means of *ex ante* regulation against teacher-student abuse. This would complement the currently inadequate measures in place and ultimately provoke more responsible behaviour from unruly university professors and members of staff, hence serving as a major deterrence against the phenomenon in Cameroon and other affected African countries in general.

[368] Sjaak Nouwt, *Reinventing data protection?* (Serge Gutwirth, Yves Poullet, Paul de Hert eds) (Preface) 2009. Ibid

**References for Chapter 4**

Agborbechem, P. T. ‘‘Sorting’ in examinations: Evaluating the quality of assessment in Universities in Cameroon.’ *International Research Journal of Arts and Social Science* Vol. 4(5) pp. 093-097, June, 2015

Bradford, A. ‘The Brussels effect.’ *Nw. UL Rev.* 107 (2012): 1.

De Hert, P & Gutwirth, S. ‘Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action.’ In *Reinventing data protection?* pp. 3-44. Springer, Dordrecht, 2009.

Floridi, L. *The Online Manifesto: Being Human in a Hyperconnected Era*. Springer Cham Heidelberg New York Dordrecht London, 2015.

Galetta, A., & De Hert, P. ‘A European Perspective on Data Protection and the Right of Access.’ In *The Unaccountable State of Surveillance*, pp. 21-43. Springer, Cham, 2017.

Gellert, R. & Gutwirth, S. ‘The legal construction of privacy and data protection.’ *Computer Law & Security Review* 29, no. 5 (2013): 522-530.

Greenleaf, G. & Georges, M. ‘The African Union’s Data Privacy Convention: A Major Step toward Global Consistency?’ 131 *Privacy Laws & Business International Report,* (2014)18--21.

Hijmans, H. ‘Understanding and Assessing the Contribution of the CJEU to the Mandate Under Article 16 TFEU.’ In *The European Union as Guardian of Internet Privacy*, pp. 185-261. Springer, Cham, 2016.

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* (2013): 1-12.

Ladkin, S. ‘Exploring Unequal Power Relations within Schools: The Authenticity of the Student Voice.’ *Journal of Initial Teacher Inquiry* 3 (2017): 37.

Makulilo, A.B. ‘“One size fits all”: Does Europe impose its data protection regime on Africa?’ *Datenschutz und Datensicherheit-DuD* 37, no. 7 (2013): 447-451.

Makulilo, A. B. ‘The Context of data privacy in Africa.” In *African Data Privacy Laws*, pp. 3-23. Springer, Cham, 2016.

Menick, M. D. 'Sexual abuse at schools in Cameroon: results of a survey-action program in Yaounde.' *Medecine tropicale: revue du Corps de sante colonial* 62, no. 1 (2002): 58-62.

Morley, L. 'Sex, grades and power: gender violence in African higher education.' In *CHEER Symposium, Annual SRHE Conference,* 14-16 December 2009. Newport, Wales.

Manyika, J.; Chui, M.; Brown, B.; Bughin, J.; Dobbs, R.; Roxburgh, C; & Byers, A.H. '*Big data: The next frontier for innovation, competition, and productivity*.' Mckinsey Global Institute. (2011).

Ngwafor, E. 'Cameroon: The Law Across the Bridge: Twenty Years (1972-1992) of Confusion.' *Revue générale de droit* 26, no. 1 (1995): 69-77.

Nouwt, S. *Reinventing data protection?*. Edited by Serge Gutwirth, Yves Poullet, Paul de Hert, and Cécile de Terwangne. Dordrecht: Springer, 2009.

Ohm, P. 'Broken promises of privacy: Responding to the surprising failure of anonymization.' *Ucla L. Rev.* 57 (2009): 1701-1777

Olivier, M. E. 'The role of African Union law in integrating Africa.' *South African Journal of International Affairs* 22, no. 4 (2015): 513-533.

Lynskey, O. *The foundations of EU data protection law*. Oxford University Press, 2015

Purtova, N. 'The law of everything. Broad concept of personal data and future of EU data protection law.' *Law, Innovation and Technology* 10, no. 1 (2018): 40-81

Rich, C. 'Privacy laws in Africa and the Middle East.' *The Bureau of National Affairs, editor. Privacy and security law report. Bloomberg: BNA* (2014).

Rouvroy, A. & Poullet, Y. 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy.' In *Reinventing data protection?* Springer, Dordrecht (2009) pp. 45-76.

Schwartz, P. M., and Solove, D. J. 'The PII problem: Privacy and a new concept of personally identifiable information.' *NYUL rev.* 86 (2011): 1814.

Stamp, M. *Information security: Principles and Practice*. John Wiley & Sons, 2011.

Wachter, S & Mittelstadt, B. D. 'A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI.' *Columbia Business Law Review* (2018).

Willott, C. ‘Factionalism and Staff Success in a Nigerian University: A Departmental Case Study.’ *States at Work: Dynamics of African Bureaucracies* (2014): 91-112.

Zoneziwoh, M. W. ‘*Sexual Violence on University Campuses: The Case of University of Buea*’. No. 2. ALC Working Paper, 2011.

## Chapter 5: 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

Accepted for presentation at and publication in upcoming EAI INTERSOL Conference 2020

**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 a legal regime to ensure that processing of personal information, especially using ICTs, follows certain rules in order to protect fundamental and human 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 around which national and supranational regimes were expected to build their personal data processing laws.

It is in this light that this paper attempts a comparative review on how these principles are consolidated in Europe and Africa: that is, between the EU's GDPR on the one hand and the Ghana and Kenyan data protection instruments on the other hand. 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 Act appears to duplicate the GDPR risk-based approach in consolidating the OECD data protection principles, the Ghanaian Act rather adopts a less rigorous approach with lesser burdens on data controllers.

**Keywords**: Data protection, GDPR, Ghana Data Protection Act, Kenyan Data Protection Act, OECD

## 5.1 Introduction

As the world keeps adopting innovations in Information and Communication Technology (ICT) and other forms of computational machinery to facilitate human interactions, the 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[369], 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.[370]

These concerns were principally privacy concerns and began following the increasing use of computational power to process information in the 1960s and 1970s[371], and it 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[372], 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 ICTs. These

[369] Daniel Solove. 'The New Vulnerability: Data Security and Personal Information. In: Anupam Chander, Lauren Gelman, and Margaret Jane Radin (eds) *Securing privacy in the Internet age*. Stanford University Press. (2008) 111. Also Xavier Caron, Rachelle Bosua, Sean B. Maynard, and Atif Ahmad.: The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review* 32, no. 1 (2016): 4-15. 6. Also see generally, Gloria Gonzales Fuster: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer Science & Business. (2014)

[370] See generally Taewoo Nam: 'What determines the acceptance of government surveillance? Examining the influence of information privacy correlates.' *The Social Science Journal* (2018).

[371] ibid

[372] Orla Lynskey: *The foundations of EU data protection law*. Oxford University Press. 2015. 1

principles later inspired the adoption of the OECD[373] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23rd September 1980 (revised on 11th June 2013), and are today generally referred to as principles of 'personal data protection' (in Europe and later Africa) or 'information privacy' (USA)[374]. They sought to provide safeguards when processing information about individuals, and especially where such processing is done by means of 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[375].

Following the above-mentioned privacy and surveillance concerns, supranational and national legal responses based on the OECD Guidelines have been developed around the globe to safeguard individuals' privacy and data protection rights within a context of ubiquitous ICT usage for personal data processing. Reason why data protection laws exist in over 120 countries worldwide including 25 African countries[376], and instruments have been introduced by international and regional institutions such as the European Union, ECOWAS[377] and the African Union[378]. 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[379] basically considers data protection as a means to guarantee the right to privacy in the information age, Lynskey[380] appears in favour of their interpretation as two separate though heavily interlinked concepts and rights, while de Hert and Gutwirth[381] acknowledge that the former was conceived to address the shortcomings of the law to guarantee the right to privacy in an increasingly digitised era; shortcomings equally observed by Solove[382]. While

[373] 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

[374] Robert Gellman. "None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive." *The George Washington International Law Review* 32, no. 1 (1999): 179.

[375] Peter Hustinx: "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* (2013): 1-12.1

[376] See Graham Greenleaf. '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 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035 Accessed 11th October 2019

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

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

[379] Francesca Bignami. "The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts." *Cornell Int'l LJ* 41 (2008): 211.224

[380] Orla Lynskey. *The foundations of EU data protection law*. 2015. Supra. 91-106

[381] Paul de Hert & Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Reinventing data protection*?, pp. 3-44. Springer, Dordrecht, 2009. 5-6

[382] Daniel Solove: '*The digital person: Technology and privacy in the information age*.' Vol. 1. NyU Press, 2004.9

acknowledging the importance of this debate in conceptualising the right to data protection, it is not the objective of this article to discuss the differences or similarities between both concepts. Nevertheless, the debate influences the adoption by this article, as a definition of data protection, the position of the Council of Europe's Convention 108 and equally as observed Hustinx[383], 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 in general how the data protection principles embedded in the OECD Guidelines are reflected 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 choice of the Ghanaian and Kenyan legislations for this comparison is two-fold: first, both countries are Common law countries and represent two sub-regional African intergovernmental organisations[384]. Secondly, and most important, both legislations represent African data protection law pre and post GDPR: the EU Regulation being adopted in 2014, hence between both selected Acts (the Ghanaian Act adopted in 2012 and the Kenyan Act adopted in 2019). So by comparing all three legislations, the article also specifically seeks to examine the influence of the GDPR on the Kenyan Data Protection Act (post-GDRP) as opposed to the Ghanaian Data Protection Act (pre-GDPR) in their consolidation of the OECD Guidelines.

This introduction shall 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, showing the effect of the GDPR on the Kenyan instrument as opposed to the Ghanaian instrument. A fifth and final section shall present the conclusive remarks.

[383] Hustinx observes: "…the Convention's approach is *not* that processing of personal data should always be considered as an *interference* with the right to privacy, but rather that for the *protection* of privacy and other fundamental rights and freedoms, any processing of personal data must *always* observe certain legal conditions". Peter Hustinx: 'EU data protection law: The Review of Directive 95/46/EC and the proposed General Data Protection Regulation.' 2013. Supra. 9.

[384] Ghana being a member of the Economic Community of West African States (ECOWAS) and Kenya a member of the East Africa Community (EAC)

## 5.2 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[385]. 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', 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[386]. 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[387]. 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.[388] In terms of scope, the Guidelines applies to any personal data which 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 defined personal data 'any information relating to an identified or identifiable individual (data subject)'[389], 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 openness principle, the individual participation principle,

[385]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

[386] Gloria Gonzales Fuster: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. (2014) supra, 76-78

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

[388] Fuster, (2016) supra, 79.

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

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.

Being the first body of data protection principles embodied in an international instrument, the OECD (Revised) Guidelines can be considered a principal foundation stone from which are constructed other data protection rules at national or regional level. It is on this basis that this paper seeks to comparatively review the consolidation of the OECD Revised Principles by the European GDPR on the one hand, and the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019 on the other hand. The following section briefly presents these selected legislations.

### 5.3 The EU GDPR[390], 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.

#### 5.3.1 The European General Data Protection Regulation (GDPR)

Coming into force on 25th May 2018 and repealing the EU 1995 Data Protection Directive[391], the GDPR is Europe's main instrument regulating the processing of personal information. 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). With the Directive serving as guidance for national data protection laws but not directly applicable on EU member states, there were concerns about the unequal levels of data protection across the EU. The GDPR was hence 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.'[392] Also, the right to data protection officially acquiring the status of a fundamental right under the 2000 EU Charter of Fundamental Rights (Article 8) warranted its consolidation under a directly applicable Regulation. The GDPR establishes rights to guarantee and obligations to comply with when processing information about or relating to individuals located within

[390] 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

[391] 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

[392] 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)

the European Economic Area, or where such processing is done by an entity located within the latter. 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[393]. It however runs concurrently with the e-Privacy Directive[394] and Police Directive[395] which apply lex specialis where the processing takes place respectively over a publicly accessible telecommunication network or within the context of a criminal investigation.

Two significant peculiarities can be identified with the GDPR. The first is what has been termed its risk-based approach to data protection i.e. it systematically requires data controllers and processors to assign more resources to processing which present greater risks to individuals in case of any processing misfortunes. Secondly, data controllers (i.e. persons responsible for the collection and processing of personal data) are the main actors in charge of the application of data protection law, with national data protection authorities playing a more or less subsidiary role[396]. In other words, it is up to data controllers to take initiatives to protect individuals whose data they are processing, while the data protection authorities are there to verify if such initiatives are adequate. The reasons for this approach, as advanced by the EU Commission, include reducing the administrative burden on data controllers[397], and that companies are in the best place to know their processing activities which could harm data subjects[398].

### 5.3.2 The Ghana Data Protection Act 2012

The Ghana Data Protection Act entered into force on 16th October 2012, with the aim to '…protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters'[399]. It was introduced to further reinforce the right to privacy guaranteed by Article 18 of the 1992 Constitution of Ghana, following the apprehension by the Government that misuse of personal information could be used

[393] Solove, Daniel: Why I Love the GDPR: 10 Reasons. Available online: https://teachprivacy.com/why-i-love-thegdpr/ (accessed on 11 October 2019)

[394] 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)

[395] 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

[396] Maria Eduarda Gonçalves: The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research*. 2019. DOI: 10.1080/13669877.2018.1517381. 2

[397] Ibid, 3

[398] Ibid, 6.

[399] Ghana Data Protection Act 2012 (title)

in a manner that is detrimental to individuals and the Ghanaian society at large[400], especially in light of technological advancements[401]. Agyei-Bekoe also asserts that another plausible if not the principal motive behind the legislation could be the desire to comply with the then trendy adequacy principle of the 1995 EU Directive (Article 25) which prohibited EU countries from making data transfers to third countries without an adequate level of privacy and (data) protection. He posits that the Ghanaian legislator was more concerned about international economic relations rather than the privacy rights of individuals, Ghana being an essentially collectivist society with people likely to have low value for privacy.[402] In any case, the Act it remains one of the first national responses by an African state to privacy and data protection concerns.

### 5.3.3 The Kenyan Data Protection Act 2019

The Kenyan Data Protection Act 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[403]. 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

[400] Dominic N Dagbanja. 'The right to privacy and data protection in Ghana.' In *African Data Privacy Laws*, pp. 229-248. Springer, Cham, 2016 .232

[401] Speech delivered by Dr. Edward K. Omane Boamah, Minister for Communications at The Launch Of The Data Protection Commission On 18th November 2014 at The International Conference Centre (Data Protection Commission). Available online at 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 11th October 2019.

[402] Eric Agyei-Bekoe: *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. 189

[403] Alex B Makulilo & Patricia Boshe: 'Data Protection in Kenya.' In *African Data Privacy Laws*, pp. 317-335. Springer, Cham, 2016.318

consists of 75 Articles arranged into 11 parts, offering a broad range of protection to Kenyan citizens with regard to personal data processing.

### 5.4 Consolidating the OECD (Revised) Principles (and corresponding rights and obligations) of data processing

This section, the main focus of this paper, reviews the consolidation 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.

#### 5.4.1 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[404] 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 (the data subject has given their consent, performance of a contract to which the data subject is party, compliance with a legal obligation, to protect the vital interests of the data subject or of another natural person; the performance of a task done in the public interest or in the exercise of official authority vested in the controller, or for the legitimate interests[405] pursued by the data controller, except where the data subject's fundamental rights override such interest).

[404] Luci Pangrazio & Neil Selwyn. 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data." *New Media & Society* 21, no. 2 (2019): 419-437.420

[405] '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)

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)).

### 5.4.2 Data Quality Principle (Paragraph 8, OECD Guidelines)

Paragraph 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. 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.[406]

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 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.

[406] 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.

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.

### 5.4.3 Purpose Specification and Use Limitation principles (Paragraphs 9 and 10, OECD Revised Guidelines)

Paragraph 9 of the OECD Revised Guidelines states that 'the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose'. And Paragraph 10 complementarily requires personal data 'not to be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except…with the consent of the data subject or…by the authority of law.' Together, both principles 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[407]. Paragraph 9 also 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.

The GDPR embeds this Principle in Article 5(b), obliging data controllers to stick to the original purpose of processing unless, inter alia, further processing is not incompatible with original purpose. Paragraph 10 of the Guidelines is materialised on its part in Article 5(e) GDPR, which requires personal

[407] Sandra Wachter & Brent Mittelstadt. "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI." *Columbia Business Law Review* (2019).4

data to be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed', exceptionally permitting their storage for longer periods 'if processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.' Also relevant in this respect is the right available to data subjects, subject to some exceptions or unless they expressly consent, not to be subject to decisions based solely on automated processing which produces legal effects concerning or affecting them (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 without prior consent.

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, unlike the GDPR, 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)).

### 5.4.4 Security Safeguards Principle (Paragraph 11 OECD Revised Guidelines)

Paragraph 11 OECD Guidelines state that 'Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.' Data controllers are therefore required to ensure that personal data is processed securely without unwanted disclosure.

The GDPR incorporates this principle in its Article 32, demanding controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [which a given processing activity could expose the individual to], including…the pseudonymisation and encryption…the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services…ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'.

On its part, Article 28(1) of the Ghanaian Act demands that the data controller takes 'reasonable, technical and organisational measures to prevent the loss of, damage to, or unauthorised destruction; and unlawful access to or unauthorised processing of personal data'. In Kenya, the Data Protection Act requires the implementation of measures to identify and maintain safeguards against risks of processing, psudonymisation and encryption of personal, and availability to restore processing in the event of a technical incident (Article 41(4)).

### 5.4.5 Openness principle (Paragraph 12 OECD Revised Guidelines)

Paragraph 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. It compels controllers to provide individuals with sufficient information on the processing being carried out[408], empowering them to scrutinize processing of their data through exercising rights like the right of access, modification and/or deletion of their processed information.

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 'provide any information…relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language…' (Article 12(1)). It equally has to be very clear about its processing objectives when obtaining the individual's consent for data processing, and should also inform them of their right to withdraw their consent at any time (Article 7 (1) to (3)). In terms

[408] See Fanny Coudert. "Towards a new generation of CCTV networks: Erosion of data protection safeguards?" *Computer Law & Security Review* 25, no. 2 (2009): 145-154.151

of rights under this principle, Article 13(2)(f) notably grants individuals the right to obtain, where automated decision-making is involved using their data, 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' on them.

In Ghana, Article 17(f) lists 'openness' as one of the principles of data processing. Article 18 requires that the controller processes personal data 'without infringing the privacy rights of the data subject…' and 'in a lawful manner'. Article 27(2) lists a rather exhaustive list of items which the controller, before collecting data for processing, must ensure the data subject is aware of. These include, inter alia, the nature of the data being collected, name and address of the person responsible for the collection, the purpose for collection, whether or not the supply of the data by the data subject is discretionary or mandatory, the recipients of the data, the existence of the right of access to and the right to request rectification of the data collected before the collection. 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. The latter 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.

### 5.4.6 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. As de Hert et al[409] generally 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. 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.

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'[410].

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 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[411]). 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.

---

[409] See Paul de Hert, Vagelis Papakonstantinou, David Wright & Serge Gutwirth S. 'The proposed Regulation and the construction of a principles-driven system for individual data protection.' *Innovation: The European Journal of Social Science Research* 26, no. 1-2 (2013): 133-144.138

[410] 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.

[411] 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

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 this 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.

### 5.4.7 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.

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 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 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).

### 5.4.8 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, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.' 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[412]. They have been asserted to serve three purposes: 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; and they force data controllers to assess and understand their own situation regarding security measures.[413]

[412] See Gina Marie Stevens. 'Data security breach notification laws.' *CRS Report for Congress* (2012). Retrieved from http://dev.journalistsresource.org/wp-content/uploads/2012/04/R42475.pdf. Accessed 13th October 2019

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

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 [414] to their data supervisory authorities, depending on the severity of the breach. Article 33(5) also compels data 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. It is important to note here that the Ghanaian Act uses the term "security compromise" without offering a definition of the term; but this remains the closest equivalent concept to a data breach under the GDPR in terms of consolidating the Security Breach notification principle. The Act, as regards reporting security incidents, does not adopt a risk-mitigating approach like the GDPR: not only does it require the reporting of (mere) "suspicions" of security com-promises, 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, the Kenyan Act, after adopting, in its Article 2, a definition of a personal data breach identical to that in Article 4(12) of the GDPR, requires notification in its Article 43(1) if a personal data breach 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.

### 5.5 Conclusive Remarks

This article set out to review how the Ghanaian and Kenyan data protection legislations fare before the European GDPR in consolidating data protection principles embedded in the 1980 OECD Guidelines

[414] 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.'

Governing the Protection of Privacy and Transborder Flows of Personal Data, including its 2013 revision. Specifically, it attempted to demonstrate the influence of the GDPR on the Kenyan Data Protection Act 2019 (post GDPR) as opposed to the Ghanaian Data Protection Act 2012 (pre-GDPR). 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 essential data protection principles around which related national or supranational legislations around the globe could be developed. The article then presents proceeds to comparatively examine the GDPR's materialisation of these principles with their materialisation in the Ghanaian Data Protection Act of 2012 and Kenyan Data Protection Act of 2019. The objective was to identify the similarities and differences between the contemporary EU approach in consolidating these principles as opposed to the approach of the selected African legislations, and by so doing, examine how the approach of the GDPR influences the Kenyan Data Protection Act 2019 (adopted post GDPR) as opposed to the Ghanaian Data Protection Act 2012 (adopted pre-GDPR). The results are illustratively summarized in the following table:

| **1980 OECD Privacy Guidelines (with 2013 amendment) principles** | **EU 2014 General Data Protection Regulation** | **Ghanaian Data Protection Act 2012** | **Kenyan Data Protection Act 2019** |
|---|---|---|---|
| Collection Limitation | - **Article 5(1)(a)**: Lawful and fair processing.<br>- **Article 5(1)(c)**: data collected should be relevant and limited<br>- **Article 6**: Lawfulness of processing | - **Article 19**: Processed data should be relevant, not excessive.<br>- **Article 20(1)**: Legal grounds for processing | - **Articles 25(b) to (d)**: Processing should be 'fair' and 'lawful'<br>- **Article 30(1)**: Legal grounds for processing |
| Data Quality | - **Article 5(d) (also Recital 39)**: Inaccurate data should be rectified<br>- **Article 16**: Right of rectification | - **Articles 17(e) and 26**: Processed data should be complete and up to date.<br>- **Article 33(1)**: Right to have inaccurate data corrected or deleted. | - **Article 25(e)**: Personal data should be accurate and kept up to date.<br>- **Article 26 (d) and (e) and 40(1)**: Right to have false information (about the data subject) corrected or deleted. |
| Purpose Specification and Use Limitation | - **Article 5(b)**: Processing should be limited to the original purpose.<br>- **Article 5(e)**: Data should not be stored for longer than necessary for processing. | - **Article 17(c)**: Specification of purpose of processing.<br>- **Article 25**: Data should be processed strictly within this specified purpose. | - **Article 25(c)**: Processing shall be for explicit, specified and limited purpose<br>- **Article 30(2)**: Processing should be strictly within specified purpose |

| | | | |
|---|---|---|---|
| | - **Article 22**: Right not to be subject to purely automated decision-making | -**Article 41(1)**: Right not to be subject to purely automated decision-making ***only*** upon a written request. | - **Article 35(1)**: Right not to be subject to purely automated decision-making |
| Security Safeguards | - **Article 32**: Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing. | -**Article 28(1)**: Take reasonable, technical and organisational measures to prevent the loss of, damage to, or unauthorised destruction; and unlawful access to or unauthorised processing of personal data | - **Article 41(4)**: Implement measures to identify and maintain safeguards against risks of processing, and restore processing in the event of a technical incident |
| Openness | - **Article 5(a)**: Transparency principle of processing.<br>- **Article 12**: Detailed processing information to be provided to data subject (including right to withdraw consent to processing) | - **Article 17(f)**: Openness as a processing principle.<br>- **Article 27(2)**: Detailed information about the processing to be made aware to data subject.<br>- **Article 41**: Notify data subject in the event of injurious automated processing. | - **Article 25(b)**: Transparency principle of processing.<br>- **Article 29**: Inform data subjects about their rights with regard to the processing.<br>- **Article 26(a)**: data subjects should be informed of the use for which their data is processed. |
| Individual Participation | - **Article 15**: Right of data subject to know if data about them is being processed, and to request access to the processed data.<br>- **Article 16-18**: Right to request rectification, erasure (right to be forgotten) and restriction of processing.<br>- **Article 20**: Right to data portability (limited to data processed by automated means) | - **Article 17(h)**: Data subject participation as a processing principle.<br>- **Articles 32 - 35**: Right of access.<br>- **Article 33(1)(b)**: Right to be forgotten.<br>- No right to data portability. | - **Article 26 (d) and (e) and 40(1)**: Right to request the correction and deletion of false or misleading data<br>- **Article 36**: Right to request restriction of processing.<br>- **Article 38**: Right to data portability (not limited to data processed by automated means). |
| Accountability and Implementing Accountability | - **Article 5(2)**: Data controller is responsible for demonstrating compliance to data protection rules.<br>- **Article 25**: Data protection by Design or by Default.<br>- **Article 35**: Data Protection Impact Assessment. | - **Article 17(a)**: Accountability as a principle of processing.<br>- No direct requirement for Data protection by Design or by Default.<br>- No direct requirement for Data Protection Impact Assessments or similar. | - **Article 41**: Data protection by Default or by Design.<br>- **Article 31**: Data Protection Impact Assessment. |
| Security breach notification | - **Article 33 and 34**: Notify severe data breaches to supervisory authorities and data subjects respectively | - **Article 31**: Data Protection Commissioner and data subject should be informed in case of 'reasonable suspicion' of a security compromise. | - **Article 43(1)**: Notification if personal data breach presents a 'real risk of harm' to the data subject. |

As illustrated in the above table, compared to the GDPR, the Ghanaian and Kenyan data protection instruments have made quite commendable effort to consolidate the OECD data protection principles to their respective citizens. As Agyei-Bekoe suggests in the case of Ghana[415], this move by African countries to adopt comprehensive data protection laws is significantly motivated by economic factors; i.e. a desire not to be left out of the European consumer market. This has been termed the "Brussels effect", term coined by Anu Bradford in 2012 to denote the regulatory influence of the EU through its institutions and standards on the rest of the world, mostly through market mechanisms[416]. Also, African legal systems are heavily influenced by European legislation, with most African states today inheriting and still using legal systems left behind by their former colonial masters after independence in the 1960s, and are hence no strangers to European law.[417] So just like the GDPR, both Ghanaian and Kenyan data protection laws feature provisions addressing data collection limitation, purpose limitation, use limitation, and include a requirement for data controllers to take measures to ensure security of processing.

However, a number of differences can be identified between the two Acts. These include, as regards the Ghanaian Act, the absence of a right to data protability, absence of a 'data protection by design or by default' requirement, no express requirement on the data controller to do a prior data protection impact assessment in the event of risky processing (the data subject has to seize the Data Protection Commissioner so the latter seizes the data controller to request n impact assessment), or the absence of an obligation to record personal data breaches. It is important to note here that the Ghanaian Act uses the term "security compromise" (rather than "personal data breach") and without offering a definition of the term; but this remains the closest equivalent concept to a data breach under the GDPR in terms of consolidating the Security Breach notification principle. The Act, as regards reporting security incidents, does not appear to 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, as is the case with the GDPR's Article 34(3). This demonstrates a difference in approach with the GDPR.

[415] See note 34

[416] See Anu Bradford. "The Brussels Effect' (2012)." Northwestern University Law Review 107 (2012): 1.

[417] For a discussion on the inheritance of European legal systems by African colonies after independence, see Sandra Fullerton Joireman. "Inherited legal systems and effective rule of law: Africa and the colonial legacy." *The Journal of Modern African Studies* 39, no. 4 (2001): 571-596. Also see Alex B Makulilo.: "One size fits all": Does Europe impose its data protection regime on Africa?. *Datenschutz und Datensicherheit-DuD* 37, no. 7 (2013): 447-451.451

Another noticeable difference is the Ghanaian Act's 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, on the other hand, consolidates the OECD Principles much more in like manner as the GDPR, literally copying the latter quite considerably. The Act adopts a similar risk-based approach in materialising the Security Breach Notification principle(requiring the reporting only of breaches which pose significant risks), places more responsibilities on data controllers as opposed to its Ghanaian counterpart by providing for a 'data protection by design' requirement as an implementation of the Accountability Principle, as well as a default right not to be subject to purely automated decisions as a means to consolidate the Use Limitation principle. And just like the GDPR, it also provides for a right to data portability to reinforce the Individual Participation principle. From the above, it can therefore be safely asserted that the 2019 Kenyan Data Protection Act, adopted five years after the GDPR, is significanly influenced by the latter in its consolidation of the OECD data potection guidelines, as opposed to the 2012 Ghanaian Data Protection Act, which came into force two years before the adoption of the GDPR. Bradford terms this development a "de jure Brussels effect," where foreign countries affirmatively adopt EU standards into their legislations.[418]

**References for Chapter 5**

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

Bignami, F. 'The Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts.' *Cornell Int'l LJ* 41 (2008): 211.

Bradford, Anu. "The Brussels Effect'(2012)."*Northwestern University Law Review* 107 (2012): 1.

[418] Anu Bradford. "The Brussels Effect' (2012).8

Caron, X.; Rachelle B., Maynard, S. B., & Ahmad, A. 'The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective.' *Computer Law & Security Review* 32, no. 1 (2016): 4-15.

Coudert, F. 'Towards a new generation of CCTV networks: Erosion of data protection safeguards?' *Computer Law & Security Review* 25, no. 2 (2009): 145-154.

Dagbanja, D. N.: The right to privacy and data protection in Ghana. In *African Data Privacy Laws*, pp. 229-248. Springer, Cham, 2016.

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: The European Journal of Social Science Research* 26, no. 1-2 (2013): 133-144.

De Hert, P. & Gutwirth, S. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Reinventing data protection*?, pp. 3-44. Springer, Dordrecht, 2009.

Fuster, G.G. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer Science & Business. (2014)

Gellman, R. 'None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.' *The George Washington International Law Review* 32, no. 1 (1999): 179

Gonçalves, M.E.: 'The risk-based approach under the new EU data protection regulation: a critical perspective.' *Journal of Risk Research*. 2019. DOI: 10.1080/13669877.2018.1517381.

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 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035 Accessed 11th October 2019

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* (2013): 1-12.

Joireman S.F. "Inherited legal systems and effective rule of law: Africa and the colonial legacy." *The Journal of Modern African Studies* 39, no. 4 (2001): 571-596

Lynskey, O. *The foundations of EU data protection law*. Oxford University Press. 2015

Makulilo, A. B. & Boshe, P. 'Data Protection in Kenya.' In *African Data Privacy Laws*, pp. 317-335. Springer, Cham, 2016.

Makulilo, Alex B.'"One size fits all": Does Europe impose its data protection regime on Africa?' *Datenschutz und Datensicherheit-DuD* 37, no. 7 (2013): 447-451

Nam, T. ‘What determines the acceptance of government surveillance? Examining the influence of information privacy correlates.’ *The Social Science Journal* (2018).

Pangrazio, L. & Selwyn, N. ‘Personal data literacies’: A critical literacies approach to enhancing understandings of personal digital data." *New Media & Society* 21, no. 2 (2019): 419-437.

Solove, D. *The digital person: Technology and privacy in the information age*. Vol. 1. NyU Press, 2004.

Solove, D. ‘The New Vulnerability: Data Security and Personal Information.’ In: Anupam, Chander; Gelman, Lauren; & Radin, Margaret Jane (eds) *Securing privacy in the Internet age*. Stanford University Press. (2008)

Solove, D. ‘Why I Love the GDPR: 10 Reasons.’ Available online: https://teachprivacy.com/why-i-love-thegdpr/. Accessed 11th October 2019.

Stevens, G.M. ‘Data security breach notification laws.’ *CRS Report for Congress* (2012). Retrieved from http://dev.journalistsresource.org/wp-content/uploads/2012/04/R42475.pdf. Accessed 13/10/2019

Wachter, S. & Mittelstadt, B. ‘A right to reasonable inferences: re-thinking data protection law in the age of big data and AI.’ *Columbia Business Law Review* (2019)

# Chapter 6: Conclusion

## 6.1 Review of background and problem questions

This thesis sought to appreciate the significance of rights and obligations under EU and African data protection law, while identifying the differences between both jurisdictions and, notably, examining the current and potential impact of EU data protection law on its contemporary African counterpart. The research interests stemmed from the background of the emergence and popularity of a relatively new right known as the right to personal data protection in Europe and the US in the 1970s and 1980s introducing and popularizing several rules regulating the processing of personal information, embedded in in national and international instruments. This coupled with Europe's capacity to export and even impose its (legal) standards and best practices on other parts of the world due to its institutional and regulatory strength as well as its lucrative market share. The research also took general interest in Europe's relationship with Africa historically engraved in colonization, European powers' pre-independence administration of their African colonies and the inheritance by the latter of the European systems of governance left behind after independence in the 1960s. Which explains the ease with which African states incorporate European contemporary standards, and lays a convenient setting for the various EU-African data protection analyses presented in this thesis.

While the right to personal data protection was first introduced to consolidate the right to privacy following the rise and unprecedented use of computerized technology to collect and process personal information by the 1970s, it has become clear that this right goes beyond protecting privacy to include protecting all individual rights as long as these rights could be at risk due to the processing of an individual's information. In other words, the right to data protection (or data protection law) is regulates the entire cycle of the processing of an individual's information in order to protect the individual from any eventual violation of all other fundamental human rights like the right to information, employment, non-discrimination, education, a fair hearing, free speech, movement, health, and even information security etc, It is in this light that this thesis focused on data protection law in Europe and Africa through an analysis of specific and relevant data protection themes: personal data security and the influence of EU data protection standards on African data protection law. The analyses made use of descriptive, exploratory and comparative methods of research, and was conducted through a number of relevant publications, which ideally constitute the chapters of the thesis. Needless to say that they represent the starting point of a future wider inquiry on the relationship between EU and African data protection law. More analytically, the thesis had a two-fold objective:

1) With a specific focus on personal security, our analysis contributes to the literature by examining what constitutes a "breach of security" under the GDPR, and discussing the state of the art of Africa's multilateral response to the personal data security concerns of the continent, in comparison with its EU counterpart

2) Focusing on selected social effect of data protection law enforcement, our analysis strove to illustrate the potential impact of EU law on African data protection law through the latter's adoption of the notion of personal data, and also by virtue of the adoption of EU standards into substantive African national data protection law.

Accordingly, the thesis posed the following research questions: What is the state of the art of personal data security law in the EU and Africa? How can EU data protection law and practice influence African national and multilateral data protection regimes? These questions were subdivided into five sub-questions, each addressed by the five publications regrouped in the thesis, as follows:

i) What are the limitations in the current definition of a personal data breach in EU law with regard to its difference with a breach of security and the protection of data subjects through breach notification? This part of the analysis focused only on European law, and involved an analysis of EU data protection legislations to determine the scope of a "personal data breach", its difference with a "breach of security" and the resulting effect of this difference on the protection of data subjects with regard to contemporary breach notification requirements.

ii) 'What is the current state of the art of Africa's multilateral response to personal data security concerns in the continent?' Response to this question led to an analysis of African personal data protection standards against those of the EU. It essentially necessitated an analysis of selected international African instruments addressing personal data security as against their EU counterparts.

iii) How can EU data protection law and practice lead to examination results be considered personal data in Africa, and what are the benefits and hindrances in implementing corresponding data protection rights on examination results within an African setting? This formed the subject matter of the first paper observing the influence of EU standards in Africa. Focusing on the domain of education, it led to an analysis of the outcome of the status of personal data being attributed to public examination results in African communities.

iv) Similarly, how can EU data protection law potentially influence the application of a data protection right of access to evaluated examination scripts in Cameroon universities, and how could this contribute to curtailing teacher-student abuses? With particular focus on Cameroon, attempting this question led us to examine personal data protection as a tool for addressing other ills of the education sector, specifically abuses in institutions of higher learning. At a time when the state is not faring so well in handling teacher-student abuse in universities, the question addressed a highly probable and perhaps revolutionary impact of EU data protection case law on the Cameroonian (and hence African) higher educational sphere in terms of regulating teacher-student abuse.

v) What are, and how has the GDPR been instrumental in the differences between the 2012 Ghanaian Data Protection Act and 2019 Kenyan Data Protection Act in their consolidation of the OECD personal data processing guidelines? This final part of our analysis was purely comparative. The question led us to strive to identify similarities and differences between the above laws, but with peculiar focus on how the differences between the selected national African Acts were influenced by the GDPR.

## 6.2 Review of analysis and findings

The first Chapter, in order to situate the limitation of the definition of a breach of security in protecting data subjects as regards breach reporting, first discusses what would constitute a 'breach of security' within the definition of a personal data breach in EU data protection law, considering the absence of a definition of the term across EU legislations. This was achieved by researching researches through scholarly literature on information security and provisions of the EU NIS Directive, with the resulting analysis then analysed in relation to rules addressing security of processing in EU data protection texts. This method revealed that in EU law, a 'breach of security' involves two eventualities: the violation of EU data protection security standards (e.g. as listed in Article 32 of the GDPR, and even without any security compromise actually happening) on the one hand, and an actual defeat of a data processing security infrastructure on another hand. The Chapter then reviews the definition of a personal data breach across EU data protection texts, which in essence considers the term to mean an a breach of security (i.e. violation of security standards or an actual defeat of a security infrastructure) system) which leads to the compromise of personal data. It makes the observation, and as reiterated by the EU Article 29 Working Party, that this definition excludes, from its scope and hence from breach notification requirements, breaches security for which no data compromise can be readily

ascertained. However, some security breaches by their very nature could be be complex or sophisticated, making the certain determination of a breach time consuming, difficult or even impossible; and excluding these from being reported simply because a data compromise cannot be ascertained by the controller could be risky for data subjects, especially where sensitive data is involved. On this premise, the Chapter proposes an alternative approach as an attempt to address this setback: inclusion of a reasonable probability (alongside certainty or confirmation) of data compromise in the substantive definition of a data breach. Or on the other hand, the notification to data subjects of security breaches which are very likely to result or have resulted in a data compromise but where such compromise is currently impossible to determine. However, notification shall remain subject to risk mitigating measures implemented on the data by the controller as provided in the notification requirements, like encryption or anonymisation.

Through descriptive and exploratory research, this Chapter contributes to clarifying the standard of what constitutes a breach of security in EU data protection law. It also presents a base from which data controllers and processors can better understand their expectations under breach reporting requirements. With all breaches of security not necessarily being personal data breaches,[419] controllers and processors can make use of this study to separate both concepts and get a better idea about when or not to report or notify a security incident to the data protection authorities or to the data subjects. Also, the Chapter could help kick-start a thought process and hence further research on the substantive definition of terms in EU data protection texts, their effects on the protection of individuals and, if need be, the exploration any alternative approaches to optimise data subject protection.

The second Chapter paper examines the response of two principal African international organisations (ECOWAS and the AU), to personal data security threats to which are (or would be) exposed African data subjects as Africa embraces ICTs and other tech-related innovations, in occasional comparison with the European response. The legislations under focus were the 2010 ECOWAS Data Protection Act and the 2014 AU Convention on Cybersecurity and Data Protection. The Chapter identified, through a literature review, some factors which may not favour the adoption and efficient implementation of personal data security norms in Africa, which include the continent's weak cybersecurity institutions, fragile privacy culture and unaccountability of its governments in maintaining satisfactory levels of human rights. It then identified and discussed current data security measures provided under the selected ECOWAS and AU legislations, observing that though these

[419] Article 29 Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018. p.7

instruments do feature some data security provisions like confidentiality and the requirement to adopt appropriate measures for secure processing, they still remained limited especially in comparison with EU data security provisions in the GDPR and even with regard to the OECD Privacy Protection Guidelines. These limitations are manifested, in both African legislations, by the absence of a requirement to report a personal data breach, lack of a Data Protection by Design provision, absence of the use of privacy certifications, as well as the absence of the establishment of a direct liability relationship between data controllers and data subjects; all of which are provided for in the EU GDPR. It is proposed here that relevant protocols be adopted within these organisations to modify these legislations and include provisions addressing these oversights.

This Chapter was researched upon for an African scientific conference bringing together many tech experts of the continent, and hence was a great opportunity to present Africa's advancements in personal data protection and security law. What motivated the research and presentation of this Chapter was principally to illustrate not only the shortcomings lack of a conceptually exhaustive framework on personal data security in Africa, but also demonstrate the apparent lack of a political will for legal integration in the continent. The comparative method of research played an essential role in demonstrating how far back the continent is as regards personal data security in relation to Europe, whose data protection standards are widely considered as the universal model for every other region or country to follow. With only five states having ratified the 2014 AU Data Protection Convention (out of the target fifteen) as of June 2020, the instrument is still a long way from becoming enforceable in all AU states.

Chapter 3 discusses the first part of the potential influence of EU case law on African data protection law. Taking cue from the decision by the ECJ (and the reasoning of its Attorney General) in the 2017 *Nowak* case, the Chapter examines the potential granting of a personal data status to academic examination results in Africa, specifically under the ECOWAS Data Protection Act and the AU Convention on Cybersecurity and Data Protection. Based on the Convention's adoption of a definition of personal data virtually identical to that of the 1995 EU Data Protection Directive, and considering Africa's historical precedence of inheriting and domesticating European law, the Chapter finds that examination results, considered personal data in Europe, can equally have the same status all over Africa when AU Convention becomes effective. In this light, the Chapter observes that a data protection status will bring along data protection rights, which will help guarantee a right to information self-determination to examination candidates, as well as limit risks of unwanted (Big data) profiling of Africans by applying the restricting unjustified further use of their examination results.

On the other hand, it identified some challenges in implementing personal data protection rights on examination results in an African context: the lack of a strong privacy culture an awareness among Africans, and the difficulty in obtaining informed consent for the further processing of candidates' results especially in rural areas. Also, the lack of privacy case law in African courts coupled with what Bakibinga terms "privacy myopia" dominating African societies would make it challenging for a candidate to bring an action in damages against an examination board or academic institution in the event of a breach leading to unauthorised access to or loss of stored but already published examination results.

Also prepared for presentation at an international tech conference in Africa, this descriptive and exploratory research was geared towards raising awareness on the personal data protection and informational privacy among African administrators and tech experts. Particularly, it is hoped that the general African public gets much more conscious about big data, and that all sorts of information they generate may be processed in ways which affect them. And no information is trivial enough to be ignored, especially information like examination results which may not only illustrate the intelligence levels of a person but also, when combined with other datasets, can infer other information like their professional orientation, religious beliefs or consumption preferences. There also was a personal attachment to the paper, with my home country Cameroon still reading and publishing public examination results (with candidates' full names and scores) on national media outlets with little regard to privacy or consideration of how this information may be used for Big Data purposes. The paper also served as a means to criticize this practice.

Chapter 4 focuses on the right of access to evaluated examination scripts in Cameroonian universities. In a follow up on Chapter 3 on the potential influence on EU case law in African data protection law, this Chapter set out to examine the possibility of the evaluated examination scripts obtaining a status of (students') personal data in Cameroon universities, and how such an eventuality could help prevent teacher-student abuses on campus. Following an analysis of the definition of personal data under the 1995 EU Data Protection Directive as adopted in more or less identical manner by the AU Data Protection Convention, coupled with the ECJ decision in *Nowak* and Cameroon's inheritance of European common and civil law, the Chapter finds that evaluated examination scripts could very likely be considered personal data under the above Convention, when it becomes effective. The Chapter then argues that this development would help in the fight against prevailing teacher-student abuse in university campuses mainly because the absence of a national law requiring universities to allow students access their evaluated scripts was a principal means for lecturers to fail

students without any means of supervision. This is also aggravated by the absence in the country of a comprehensive national Code of Ethics binding university lecturers. However, in the absence of any national laws to the contrary, students would be able to exercise a data protection right of access under Article 17 of the AU Convention to access their evaluated examination scripts, once the Convention comes into force. This development would discourage defaulting lecturers and encourage transparency in evaluations, hence contribute to limit incidents of teacher-student abuse. The Chapter however identifies two possible hindrances in guaranteeing this right to students. First, there is the possibility of a power clash between the Cameroon Data Protection Authority (DPA) and university administration in enforcing the right of access, as a DPA's order to have an evaluated script produced may be against university rules. And secondly, the immunity of campuses of higher education from interference by law enforcement authorities could hinder the investigations of a DPA who may want to investigate a complaint by students regarding the refusal of their right of access to their evaluated examination scripts.

This Chapter has as main motivation to demonstrate the importance of personal data protection as an instrument of social regulation. Away from automatic processing of personal data and other tech-related privacy concerns for which it was originally conceived, data protection as a fundamental right has evolved to be of significant service in situations which have very little to do with technology. By making a case for the adoption of EU standards of interpreting personal data protection law into Cameroon (and Africa as a whole) to solve social problems within the country, the Chapter also demonstrates the benefits of comparative law in through legal transplant.

Chapter 5 had as objective to explore the influence of the GDPR on national African data protection laws, and set out to achieve this through a comparative analysis between the GDPR, the 2012 Ghanaian Data Protection Act and the 2019 Kenyan Data Protection Act in consolidating data protection principles embedded in the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, including its 2013 revision. It sought to identify similarities and differences in how all three selected legislations materialize the OECD principles, while showing, in the process, how the GDPR influences the Kenyan Data Protection Act 2019 (adopted post GDPR) as opposed to the Ghanaian Data Protection Act 2012 (adopted pre-GDPR). Compared to the GDPR, the Ghanaian and Kenyan data protection instruments have made quite commendable effort to consolidate the OECD data protection principles to their respective citizens. As Agyei-Bekoe suggests

in the case of Ghana[420], this move by African countries to adopt comprehensive data protection laws is significantly motivated by economic factors; i.e. a desire not to be left out of the European consumer market. This has been termed the "Brussels effect", coined by Anu Bradford in 2012 to denote the regulatory influence of the EU through its institutions and standards on the rest of the world, mostly through market mechanisms[421]. Also, African legal systems are no strangers to European law; African states actually inherited European legal systems left behind by their former European colonial masters after independence in the 1960s. Similarities between their legal approaches to a global issue like personal data protection could therefore be expected. This is demonstrated in this article as, like the GDPR, both Ghanaian and Kenyan data protection laws feature provisions addressing data collection limitation, purpose limitation, use limitation, and include a requirement for data controllers to take measures to ensure security of processing.

However, a number of differences can be identified between the two Acts, with some measures missing from the Ghanaian Act but present on both the GDPR and the Kenyan Act. These include, as regards the Ghanaian Act, the absence of a right to data protability, absence of a 'data protection by design or by default' requirement, no express requirement on the data controller to do a prior data protection impact assessment in the event of risky processing (the data subject has to seize the Data Protection Commissioner so the latter seizes the data controller to request n impact assessment), or the absence of an obligation to record personal data breaches. Also, in the event of a breach, it does not appear to limit reporting only of breaches which pose a (significant) risk to data subjects or if measures have been taken to adequately minimise the damage, as is the case with the GDPR's Article 34(3). This demonstrates a difference in approach with the GDPR, and consequently the Kenyan Act.

The Kenyan Data Protection Act, on the other hand, contains the above data processing measures in very like manner with the the GDPR. It adopts a similar risk-based approach in materialising the Security Breach notification principle by requiring the reporting only of risky data breaches breaches, and provides for the recording of data breaches. Significantly, it adopts an identical definition of a personal data breach as the GDPR, and features a 'data protection by design' requirement, and right to data portability, just like the GDPR. These illistrate that the GDPR has significant influence in the standards set by the Kenyan data protection legislator, as opposed to the Ghanaian standards which were adopted pre-GDPR.

[420] See Chapter 1 (Introduction) note 34
[421] See Anu Bradford. "The Brussels Effect'." Northwestern University Law Review 107 (2012): 1.

Also prepared for an African tech conference in Nairobi, this Chapter was conceived, in the first place, to raise general awareness among African tech experts on globally-recognised personal data protection principles. Also, measuring the EU data protection system against African national laws serves as a means to illustrate the fragmented levels of data protection among African states, which could be a significant hindrance to the international free flow of personal data within the continent. The Chapter is thus expec"ted to provoke awareness among tech experts of this discrepancy so they may pressurise policy makers to push for better harmonisation and integration of data processing laws among African states.

### 6.3 Final observations and further research

Personal data protection law has been documented to offer significant benefits to society in the wake of technological innovations which process information about individuals.[422] Concieved in the US and Europe in the early 1970s to consolidate the right to privacy amidst the introduction and increasing use of computational power to automatically process and share persinal information and vast surveillance, this relatively new branch of law birthed certain rights and obligations aimed at ensuring that such information is processed in ways which may not negatively affect the privacy of the individuals to whom they relate. Some of these rules as have been developed over the years include consent before processing, limited storage of personal information to only when strictly necessary, no further processing to infer new information from information already acquired unless such processing is consented to, processing should have justifiable legal grounds, and processing should be secure. While this branch of law initially targeted the right to privacy, perhaps one of its peculiar characteristics is its ability to affect all forms of fundamental rights attributed to humans in relevant international instruments, as long as these rights may be affected by information processing. In other words, besides the right to privacy, data protection can be involved to protect a person's right to a fair trial[423], protect our right to employment by ensuring accuracy of personal data within job search websites,[424] or other rights which could be at risk through misuse of personal information, and which

[422] See generally Gloria González Fuster. *The emergence of personal data protection as a fundamental right of the EU*. Vol. 16. Springer Science & Business, 2014; Paul de Hert &Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Reinventing data protection?*, pp. 3-44. Springer, Dordrecht, 2009.

[423] See for example the critique of the use of the software COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) in US courts to calculate the chances of recidivism of accused persons. To decide on recidivism risk, the software took in account the age of the accused, arrest history, vocation education etc. Following a study in May 2016, it was asserted that the algorithm was biased against black people than whites. See Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner**. "**Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks." *ProPublica.* May 23, 2016. Available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing Accessed 5th June 2020

[424] Spokeo Inc. v. Robins, 742 F.3d 409 (9th Cir. 2014

may not always fall within the traditional right to privacy. It is with these findings that this research explored, besides normative personal data securtiy issues within the EU and Africa, the potential benefits which personal data protection law could offer to the average Africans.

This research led us to examine the origins of personal data protection law and privacy particlarly in the EU and US, the extraterritorialy of EU (data protection law) and the legal relationship between Africa and Europe. By comparing the levels of personal data protection in the EU and Africa, as well as examining the possibilites of transposing EU data protection standards into African legal practice, the research concludes on two principal findings. Firstly, there is a lot still to be done in Africa in terms of reaching a harmonised framework for personal data protection and data security among states, which seems a reflection of the lack of political will for legal integration as well as the absence of a privacy culture in Africa. And secondly, transposing EU data protection standards into Africa could be a convenient starting point to consolidate a privacy and/or data protection consciousness and culture, promote information self determination and even solve social problems like sexual harrassment in university campuses. Needless to say, any transposition needs to come with efficient enforcement institutions. This would translate into the establishment and staffing of data protection supervisory authorities, imposing the appointment of data protection officers in organisations processing large amounts of personal data and, considering the lack of privacy case law in the continent and hence lack of expertise of our judiciary system, educating and sensitising national judgdes on data protection and tech regulation in general.

As regards further lines of research, this work makes it evident that the benefits of personal data protection are very vast, with the ability to stretch its effects to affect a wide variety of domains in as much as they involve human activity. The principles of personal data processing set by the OECD for example could be researched further to understand and suggest where they can serve as additional protection for Africans where other branches of law are lacking. Just as the right of access has been demonstrated in this thesis to be potentially able to help protect students against lecturer abuse in African universities, we remain positive that the prevalence of other societal ills may be curtailed with the help of well-researched data protection principles within national our administrative and governance projects. We therefore intend to launch future research projects into exploring how personal data protection can address other societal problems in Africa or complement other laws in their regulatory tasks where these laws are limited in scope or rationae materiae jurisdiction.

**References for Conclusion**

Bradford, A. “The ‘Brussels Effect.’ Northwestern University Law Review 107 (2012)

De Hert, P. & Gutwirth, S. "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action." In *Reinventing data protection?*. pp. 3-44. Springer, Dordrecht, 2009.

Fuster, G.G. *The emergence of personal data protection as a fundamental right of the EU*. Vol. 16. Springer Science & Business, 2014.