ENHANCING DATA PROTECTION IN KENYA: EVALUATING THE AMBIGUITIES IN DATA RETENTION POLICIES AND THEIR IMPACT ON PRIVACY AND SECURITY

Prepared as part of the requirements for earning the Bachelor of Laws Degree at Strathmore University Law School.

Authored by:

GRACE RIVIA NYAWIRA WACHIRA

112120

Researched under the supervision of

Sussie Mutahi

March, 2025

Word Count: 24,367

TABLE OF CONTENTS

ACKNOWLEDGMENT

With deep gratitude, I praise the Almighty for blessing me with the knowledge, wisdom, health, determination, perseverance and passion needed for this research. I extend my heartfelt thanks to my mother for the tremendous sacrifices and unwavering support in helping me grow and achieve my goals.

DECLARATION

I, GRACE RIVIA NYAWIRA WACHIRA, hereby declare that the work presented in this document is my own original research and has not been completed by any other person. I affirm that no part of this work has been plagiarized and that all sources of information have been duly acknowledged. This work is a result of my own effort and dedication to this field of study. Other works cited or referenced are accordingly acknowledged.

Signed: 

Date: 12-05-25

This dissertation has been submitted with my approval as University Supervisor

Signed: 

Date: 05-05-25

Supervisor's Name:

LIST OF ABBREVIATIONS

NAME	ABBREVIATION
Data Protection Act 2019	DPA
European Court of Human Rights	ECHR
Restricted Access/ Limited Control Theory	RALC
General Data Protection Regulation	GDPR
International Covenant on Civil and Political Rights	ICCPR
Universal Declaration of Human Rights	UDHR
National Integrated Identity Management System	NIIMS
Telecommunications Act	TKG
Office of the Data Protection Commissioner	ODPC
The European Court of Justice	ECJ
Telecommunications Act	TKG
Court of Justice of the European Union	CJEU
Federal Data Protection Act	BDSG
Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten	TDDDG

LIST OF CASES

Kenyan Case Law

Jesse Othoo v Safaricom Limited (2022) eKLR

Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government (2017) eKLR

Julius Karanja v. National Police Service & 3 Others (2021) eKLR

Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others (2016) eKLR

Kituo Cha Sheria & 8 others v The Attorney General (2013) eKLR

Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) (2020) eKLR

ODPC Complaint No 677 of 2022 (Office of the Data Protection Commissioner, Kenya)

Okiya Omtatah Okoiti v. Attorney General & 2 others (Petition No. 5 of 2019) eKLR

Okiya Omtatah Okoiti v Communication Authority of Kenya and Others (Constitutional Petition No. 53 of 2017)

Okiya Omttatah Okoiti v Communications Authority of Kenya & 8 Others (2018) eKLR

Okoth Ochieng v Safaricom (2021) eKLR

Raila Amolo Odinga & another v Independent Electoral and Boundaries Commission & 2 others (2017) eKLR

Rev Dr Timothy M Njoya & 6 others v The Hon Attorney General & 4 others (2004) eKLR

Foreign Case Law

1 BvR 256/08 (Judgment of the First Senate of 2 March 2010) – Germany

Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH (1 Sep 2022) – Germany

Digital Rights Ireland Ltd. v. Ireland (Judgment, 8 Apr 2014) – European Court of Justice (ECJ)

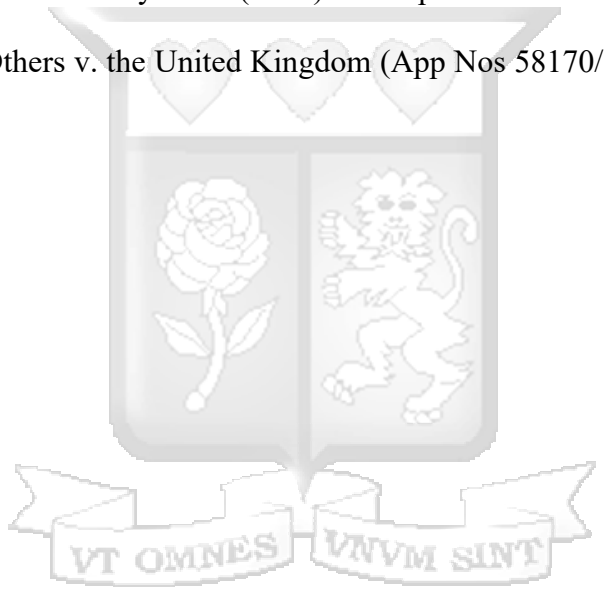
Directive 2006/24/EC (European Union)

Google LLC v CNIL (C-507/17) – European Court of Justice (ECJ)

R v Secretary of State for the Department of Interior (C-553/07) – European Court of Justice (ECJ)

Tele2 Sverige AB v. Post- och telestyrelsen (2014) – European Court of Justice (ECJ)

Big Brother Watch and Others v. the United Kingdom (App Nos 58170/13) – European Court of Human Rights (ECHR)



LIST OF LEGAL INSTRUMENTS

Banking Act 1989, Cap 488

The HIV and AIDS Prevention and Control Act No. 14 of 2006

The Kenya Information and Communications (Consumer Protection) Regulations (2010)

Universal Declaration of Human Rights (UDHR)

International Covenant on Civil and Political Rights 1966

Registration of Persons Act, 2022, Cap 170

Data Protection (Civil Registration) Regulations, 2020

Data Protection (Complaints Handling Procedure & Enforcement) Regulations, 2021

Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021

CHAPTER ONE

INTRODUCTION TO THE STUDY

1.1 BACKGROUND

The President signed into law the Kenya Data Protection Act, 2019 on 8th November 2019.[1] The Data Protection Act is an answer that aimed at ensuring Kenyans were empowered with enforceable privacy rights over their personal information, while providing clear guidelines for private and public institutions to handle their users' data with care, due to the increased call for protection of both personal and private information, which may be readily and easily accessible in this digital era.[2] The Act regulates how data and information may be accessed, processed, stored, transmitted, and used within legal parameters in Kenya. In this digital era, data and information are vital in driving the global economy; thus, data is an emerging resource that must be carefully utilised and protected.[3] The Data Protection Act outlines the principles of data protection in Kenya and is modelled on the principles set out in the EU General Data Protection Regulation which is the EU law on data protection and privacy.[4]

The Data Protection Act in Kenya aims to uphold the right to privacy as outlined in Article 31(c) and (d) of the Constitution.[5] It establishes the Office of the Data Protection Commissioner to oversee the regulation of personal data processing, articulate the rights of data subjects, and outline the responsibilities of Data Controllers and Data Processors.[6] The Act mandates that personal data processing must adhere to key principles, including the right to privacy, lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, and storage limitation.[7] Importantly, it specifies that personal data should not be retained longer than necessary for the

---

[1] *The Kenya Data Protection Act*, (No. 24 of 2019).
[2] Riofrio J, 'The Natural Law Formula and the Missing Link: Tracing and Updating Aquinas' Methodology' *Forum Prawnicze,* 2022, 5-31, https://ssrn.com/abstract=4439018 on December 1, 2022.
[3] Christopher G. Bradley, 'Privacy for Sale: The Law of Transactions in Consumers' Private Data' *Yale Journal on Regulation,* 2023, 127-212, https://openyls.law.yale.edu/bitstream/handle/20.500.13051/18236/Christopher%20G.%20Bradley%20Privacy%20for%20Sale%20The%20Law%20of%20Transactions%20in%20Consumers%20Private%20Data%2040%20Yale%20J.%20on%20Regul.%20127%20(2023).pdf?sequence=1&isAllowed=y[1]
[4] Gordon S and Ram A, 'Information wars: How Europe became the world's data police' Financial Times, 2018, https://www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8 on 20 May, 2018.
[5] Article 31, *Constitution of Kenya, (2010)*.
[6] Section 18, *The Kenya Data Protection Act*, (No. 24 of 2019).
[7] Section 25, *The Kenya Data Protection Act,* (No. 24 of 2019).

purposes it was collected for unless lawful reasons justify extended retention.[8] Despite these provisions, Section 39 of the Act lacks specificity regarding data retention durations, allowing Data Controllers and Processors to keep data for as long as deemed reasonable and necessary.[9] The case Nubian Rights Forum & 2 others v Attorney-General, the court highlights the necessity of a comprehensive legal, regulatory, and institutional framework for effective personal data protection. This ambiguity poses significant concerns about data privacy and security, as it can lead to inconsistent data handling practices and increased risks of unauthorized access, misuse, and data breaches when retained for longer periods after its use has elapsed.

Furthermore, the Act provides robust rights to data subjects, including the right to access, rectify, and object to the processing of their personal data.[10] It also includes stringent measures for the protection of children's data[11] and safeguards against the transfer of personal data outside Kenya without adequate protection.[12] This paper aims to investigate the implications of the undefined data retention period in Kenya's Data Protection Act, focusing on potential risks and proposing clear guidelines to enhance data protection practices. By comparing with Germany, which has specific data retention laws under the Telecommunications Act (TKG) requiring data storage for ten weeks and location data for four weeks, with irreversible deletion mandated within a week after the retention period.[13] This study seeks to develop best practices for data retention that ensure compliance and safeguard personal information.

1.2 STATEMENT OF PROBLEM

The lack of a prescribed duration for data retention under Section 39 of the Act, which allows Data Controllers and Data Processors to retain personal data for as long as deemed reasonable and necessary, presents a significant area of concern. This research aims to explore the implications of this ambiguity on data privacy and security, specifically examining how different interpretations of "reasonable and necessary" affect the protection of personal data. The study will focus on identifying potential risks associated with indefinite data retention, such as unauthorized access,

---

[8] Section 39, *The Kenya Data Protection Act*, (No. 24 of 2019).
[9] *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others* eKLR.
[10] Section 26, *The Kenya Data Protection Act*, (No. 24 of 2019).
[11] Section 33, *The Kenya Data Protection Act*, (No. 24 of 2019).
[12] Section 48, *The Kenya Data Protection Act*, (No. 24 of 2019).
[13] Section 175, *Telecommunications Act (TKG),* (2004).

misuse of data, and data breaches. It will also investigate how these practices impact individuals' trust in data-handling entities and the overall efficacy of data protection regulations.

1.3 RESEARCH OBJECTIVES

1. Examine the risks of indefinite data retention and the need for clear guidelines to ensure effective data protection.
2.Analyze Germany's jurisdictional framework regarding data retention practices, focusing on the compatibility of its laws with EU regulations and the European Court of Justice rulings on national data retention policies.
3.Propose Clear Guidelines by comparing with other jurisdictions like Germany, which has specific data retention laws under the Telecommunications Act (TKG)

1.4 RESEARCH QUESTIONS

1.What are the risks associated with indefinite data retention under Section 39 of the Data Protection Act?
2.How do Data Controllers and Data Processors interpret "reasonable and necessary" in the context of data retention Germany's jurisdiction?
3.What guidelines and best practices can be proposed to improve data retention policies in Kenya?

1.5 JUSTIFICATION OF STUDY

Data privacy protections benefit everyone. They empower individuals, shield marginalized groups, protect the general public, build trust for businesses, and promote a fairer digital society. It's crucial to balance privacy with proportionality and ensure vulnerable groups are protected.[14] The DPA is still in its early stages, but there's hope it will start addressing current data challenges and boost accountability among the government, private companies, and individuals. This paper will show that indefinite data retention will impact individuals' trust in data-handling entities and the overall efficacy of data protection regulations.
Despite the implementation of the Data Protection Act (DPA) bringing clarity to certain aspects of data security, it remains flawed in certain areas. Although the Act strives to safeguard individual

[14] Riofrio J, 'The Natural Law Formula and the Missing Link' 19.

privacy and regulate personal data processing, it falls short of fully realizing these objectives. Specifically, the Act lacks a prescribed duration for which Data Processors and Data Controllers may retain personal data. According to Section 39, Data Controllers and Data Processors are permitted to retain personal data for as long as it is deemed reasonable and necessary to fulfill the intended purposes of its collection. Consequently, Data Controllers and Data Processors may retain personal data for the necessary duration to accomplish their objectives.

Data Controllers and Data Processors may retain personal data beyond the fulfillment of their initial purposes, provided they can demonstrate legal authorization for such retention. However, personal data should only be retained for legitimate and lawful purposes, and only after obtaining the Data Subject's consent. Additionally, Data Controllers and Data Processors must adhere to a prescribed retention period, ensuring personal data is not kept indefinitely. They are required to dispose of personal data once the purpose for its collection has been accomplished, or when the retention period has expired.

1.6 HYPOTHESIS

The absence of a prescribed data retention duration under Section 39 of the Kenya Data Protection Act, which permits Data Controllers and Data Processors to retain personal data for as long as it is deemed reasonable and necessary, leads to significant variability in data handling practices. This lack of specificity creates a grey area in data protection, resulting in potential inconsistencies and vulnerabilities. Different interpretations of reasonableness among Data Controllers and Data Processors contribute to a fragmented approach to data retention, which increases the risk of unauthorized access, data misuse, and breaches. These risks are exacerbated by the indefinite nature of data retention, making it challenging to ensure the security and privacy of personal information over extended periods.

This ambiguity in retention policies undermines the trust of individuals in entities responsible for their data, as they remain uncertain about how their personal information is managed and protected. The potential for prolonged data retention without clear guidelines also poses challenges for regulatory compliance and enforcement, further diminishing the effectiveness of data protection measures.

Therefore, this research hypothesizes that the implementation of specific and standardized data retention durations within the framework of the Data Protection Act will mitigate these risks. By establishing clear, uniform guidelines for data retention, it is anticipated that data handling practices will become more consistent, thereby enhancing data security and reducing the likelihood of data breaches. Moreover, such measures are expected to bolster public trust in data-handling entities, as individuals gain greater confidence in the safeguarding of their personal information. This, in turn, will lead to improved compliance with data protection regulations and contribute to the overall efficacy of data protection efforts in Kenya.

1.7 THEORETICAL FRAMEWORK

1.71 The Restricted Access/ Limited Control Theory

Moor introduced this theory in 1997, blending structural and individualistic ideas of privacy. Herman Tavani and Moor further expanded it in 2001. Here, privacy is defined as shielding people from natural intrusions or observations while simultaneously maximizing their personal choices.[15] The Restricted Access/ Limited Control Theory (RALC) assumes that a solid privacy theory must separate the concept of privacy from its justification and management. These three elements constitute the RALC framework. When examining privacy, RALC differentiates between the state of having privacy (the necessary factors for privacy) and the right to privacy.[16] This distinction helps us separate the concepts of losing privacy and violating privacy. According to RALC, a person enjoys privacy in a given situation with respect to others if they are shielded from intrusion, interference, and access to their information by others in that context.[17] This 'situation' can range over various states of affairs that we regard as private, for instance, relationships, a place and even information that has been input into a computer. If in that situation, one is naturally protected or

[15] Moor J, 'Towards a theory of privacy in the information age' 27 *ACM SIGCAS Computers and Society* 3, 1997, 27–32.
[16] Tavani H, 'Philosophical theories of privacy: Implications for an adequate online privacy policy' 38 *Metaphilosophy* 1, 2007, 1–22.
[17] Moor J, 'Towards a theory of privacy in the information age', 30.

shielded from intrusion or interference and access by others, one can say that he has natural privacy.[18]

This 'situation' can encompass various scenarios we consider private, such as relationships, locations, or data entered into a computer. If, in these scenarios, a person is naturally protected from intrusion, interference, and unauthorized access by others, it can be said they have natural privacy.

RALC identifies two types of situations: naturally private and normatively private.[19] Naturally private situations occur when individuals are protected from observation, interference, and intrusion by natural means, such as physical boundaries in natural settings.[20] In these instances, privacy can only be lost. On the other hand, normally private situations are protected by laws, conventions, and norms, making it possible for privacy to be both violated and lost. [21]

By emphasizing restricted access and limited control over personal data, RALC underscores the need for clear guidelines on data retention periods. It argues that indefinite data retention without specified limits can lead to unauthorized access, misuse, and breaches, ultimately eroding individuals' privacy. Thus, implementing defined retention periods aligns with the principles of RALC, ensuring that personal data is protected and individuals' rights to privacy are upheld. This theoretical framework supports the need for specific, standardized data retention durations to mitigate risks and enhance data protection practices. It reinforces the argument that clear, enforceable guidelines are essential for maintaining trust in data-handling entities and ensuring the efficacy of data protection regulations.

1.8 LITERATURE REVIEW

Current academic literature revolves around consent being the cornerstone of the personal data privacy regime.[22] Onora O'Neill has remarked the doctrine of consent as based on the principles of individual autonomy, dignity, and integrity. It is founded on a fundamental respect for

[18] Moor J, 'The Ethics of Privacy Protection' 39 *Library Trends* 1–2, 1990, 69–82.
[19] Moor J, 'The Ethics of Privacy Protection' 77.
[20] Moor J, 'The Ethics of Privacy Protection' 77.
[21] Moor J, 'The Ethics of Privacy Protection' 77.
[22] Organisation for Economic Co-operation and Development, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], 11 July 2013.

individuals and closely linked to the right to privacy.[23]Consent from participants, as data subjects, dictates the responsibility and accountability of data users. Traditionally, consent must be obtained individually, for a specific purpose.[24] With the advancement of data mining and big data technologies, the potential risks and harms related to subsequent data use may not be evident at the time when the data is initially collected and utilized.

Thomas Ploug and Soren Holm incorporate dynamic consent, broad consent, blanket consent, and blanket refusal into the concept of meta consent. These different types of consent are introduced to the data subject at the initial point of data collection, enabling them to decide how and when they wish to give additional consent for future research. Essentially, the data subject chooses the type of consent they want to provide for various research purposes. This choice requires that the researcher disclose the different types of research that might use the subject's personal information.[25]

Goldfarb and Catherine Tucker[26] explore how privacy regulations affect data-driven innovation. They contend that advancements in information and communication technology have simplified and reduced the cost for companies to gather detailed and potentially intrusive information about their customers.[27] This shift has highlighted privacy issues, extending concerns beyond just government surveillance and the private lives of public figures.[28] Scholars have extensively discussed the necessity for a framework that advocates for privacy and consent, highlighting various aspects that need comprehensive attention.

In summary, the prevailing academic discourse underscores the pivotal role of consent in personal data privacy frameworks. The principles of individual autonomy, dignity, and integrity, as highlighted by Onora O'Neill, form the bedrock of consent doctrine, closely aligning with the right to privacy. The evolution of consent practices, particularly the concept of meta consent proposed by Thomas Ploug and Soren Holm, reflects the need for more adaptive and dynamic approaches

---

[23] Beauchamp T L and Childress J F, *Principles of Biomedical Ethics*, 7th ed., Oxford University Press, New York, 2012, 107.

[24] Kuehn B M, 'Groups Experiment with Digital Tools for Patient Consent' 310 J*ournal of the American Medical Association* 7, 2013, 678–679.

[25] Holm S and Ploug T, 'Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research' 30 *Bioethics* 9, 2016, 721–732.

[26] Goldfarb A and Tucker C, 'Privacy and Innovation' 12 *Innovation Policy and the Economy* 1, 2012, 65–90.

[27] Goldfarb A 'Privacy and Innovation', 2012, 65.

[28] Goldfarb A 'Privacy and Innovation', 2012, 65.

in response to the complexities introduced by data mining and big data technologies. Moreover, Goldfarb and Catherine Tucker's exploration of the interplay between privacy regulations and data-driven innovation emphasizes the importance of establishing robust frameworks that balance privacy protection with technological advancements. This paper reveals a critical gap in addressing the practical implications of data retention policies, setting the stage for further research aimed at developing comprehensive guidelines that protect personal data while accommodating the evolving landscape of data technology.

1.9 RESEARCH METHODOLOGY

The research will use a doctrinal approach, it will employ a doctrinal research approach, focusing on both primary and secondary data sources to examine the risks of indefinite data retention and analyze Germany's jurisdictional framework regarding data retention practices. Primary sources will include legal documents such as the Charter of Fundamental Rights of the European Union, the Universal Declaration on Human Rights (UDHR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), the International Covenant on Civil and Political Rights (ICCPR), the Data Protection Act, 2019 (Kenya), Germany’s Telecommunications Act (TKG), and European Court of Justice rulings on national data retention policies. These documents will be accessed through official government websites, legal databases (EUR-Lex, LexisNexis), and international human rights platforms. Secondary sources will encompass academic publications, studies, legal articles, reports, policies, and textbooks sourced from academic journals, reports from organizations like the European Data Protection Board (EDPB) and the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), and online databases such as JSTOR, Google Scholar, and HeinOnline. Data will be collected through library research, online searches, and document analysis, and then analyzed to assess the implications of indefinite data retention on privacy rights and security, as well as evaluate how German laws align with EU regulations and ECJ rulings, highlighting areas of compliance and potential reform. This study will provide a thorough analysis of the evolving legal issues and laws to assess how well Kenya has complied with these instruments and suggest ways for Kenya to effectively implement its data protection regulations.

1.10 RESEARCH LIMITATION

While this study will undoubtedly offer valuable insights through its doctrinal analysis of legal instruments, it's important to acknowledge the inherent limitations of this methodology. The focus on legal text can provide a strong foundation, but it might not fully capture the real-world impact of data protection laws in Kenya. Social, economic, and technological factors influencing data protection practices could be overlooked. Additionally, the interpretation of legal materials can influence the analysis, potentially leading to varying conclusions depending on perspective. Furthermore, this approach doesn't incorporate data from individuals or organizations, which could limit understanding of how effectively regulations are implemented or the challenges faced by stakeholders. By being aware of these potential limitations, the study can strive to present a more comprehensive picture by potentially including supplementary sources like reports on data protection implementation or exploring public awareness through non-doctrinal methods.

1.11 CHAPTER BREAKDOWN

Chapter 1

This chapter introduces the dissertation. It outlines the background of the study. It lays out research objectives and research questions. It also comprises a problem statement that clearly outlines the problem that this paper seeks to tackle. The theoretical framework analyzes certain theories that help in the understanding of the research problem. Research Methodology outlines the way in which the paper is to be carried out, including the methods of research and data gathering that are to be applied so as to answer the research questions and objectives.

Chapter 2

This chapter delves into the risks associated with indefinite data retention under Section 39 of the Data Protection Act. This chapter will explore how the lack of a prescribed retention duration leads to potential data privacy and security issues, such as unauthorized access, data misuse, and breaches. By examining these risks through case studies and real-world examples, the chapter aims to highlight the consequences of indefinite data retention and emphasize the need for clear, enforceable guidelines to protect personal information and ensure compliance with data protection regulations.

Chapter 3

This chapter aims to uncover the variations in data retention practices across Germany and Kenya and analyze the factors influencing these interpretations. Through case studies, the chapter will provide insights into how these interpretations impact data privacy and security, highlighting the need for more standardized guidelines to ensure consistent and effective data protection practices.

Chapter 4

This chapter will focus on proposing guidelines and best practices to improve data retention policies in Kenya. This chapter aims to develop actionable recommendations based on a comprehensive analysis of data retention practices and the challenges identified in previous chapters. By drawing insights from comparative studies with other jurisdictions like Germany, the chapter will identify best practices that can be adapted to the Kenyan context. It will provide clear, standardized guidelines designed to enhance data protection compliance, improve data security, and build public trust in data-handling practices. The goal is to offer practical solutions that address the current ambiguities in data retention under the Data Protection Act.

CHAPTER 2

LEGAL FRAMEWORK OF THE KENYA DATA PROTECTION ACT

2.1 Introduction

Data retention refers to the practice of storing and managing data for a specific period to meet various operational, legal, and regulatory requirements.[29] In the digital era, where vast amounts of personal data are continuously generated and processed, effective data retention policies are crucial for ensuring that personal information is handled responsibly and securely.[30]

The importance of data retention in data protection cannot be overstated. Properly managed data retention policies help protect individuals' privacy by limiting how long personal data is kept,

[29] Goddard M, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' International Journal of Market Research, 201, 703–705 - https://doi.org/10.2501/IJMR-2013-060 , published 2013.

[30] Bygrave L A, 'International Data Privacy Codes' in Bygrave L A (ed) *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014, 45–67.

thereby reducing the risk of unauthorized access, misuse, and data breaches.[31] They also ensure compliance with legal and regulatory requirements, helping organizations avoid penalties and build trust with customers and stakeholders.[32] Additionally, clear data retention guidelines provide a framework for data disposal, ensuring that obsolete or unnecessary data is securely deleted, further mitigating potential security risks.[33]

2.2 The Kenyan Data Protection Act (DPA)

Section 39 of Kenya's Data Protection Act addresses the retention of personal data by Data Controllers and Data Processors.[34] This section permits the retention of personal data for as long as it is deemed "reasonable and necessary" to fulfill the purposes for which it was collected. However, it does not prescribe specific retention durations, leading to ambiguity and varied interpretations among organizations .[35]

The lack of a clearly defined retention period in Section 39 poses significant challenges. Without explicit guidelines, Data Controllers and Data Processors may adopt inconsistent data retention practices, potentially increasing the risk of data privacy and security issues. This ambiguity can result in the prolonged retention of personal data, heightening the chances of unauthorized access, misuse, and breaches.[36] Consequently, there is a growing need for more precise data retention guidelines to enhance compliance, protect personal information, and build public trust in data-handling practices.[37] In this chapter, we will delve deeper into these issues, examining the risks associated with indefinite data retention under Section 39 and exploring the necessity of clear, enforceable guidelines to ensure effective data protection.

---

[31] Solove D J, 'A Taxonomy of Privacy' University of Pennsylvania Law Review, 2006, 477–560, https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/ January, 2006.

[32] 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), OJ L 119, 4 May 2016.

[33] Information Commissioner's Office (ICO), Guide to the General Data Protection Regulation (GDPR), 2019.

[34] *The Kenya Data Protection Act, (No. 24 of 2019).*

[35] Odhiambo, E, 'Privacy and Data Protection in Kenya: Evaluating the Implementation of the Data Protection Act', *East African Law Journal*, p. 45-67.

[36] Custers B, 'The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology', Tilburg University, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3186639, 2016.

[37] Mugambi M, 'Data Protection Compliance in Kenya: Evaluating the New Regulatory Landscape' *Journal of Data Protection and Privacy*, 2021, 131–145 - https://www.henrystewartpublications.com/jdpp/v4 2021.

2.3 Tension Between Privacy and Security Under the Data Protection Act

The conservation of indefinite data refers to the practice of archiving personal data for an unspecified period of time, often without the informed consent of the data subjects or a clear logic. Pursuant to the data protection law, the conservation of personal data must be limited to what is necessary for the purposes for which the data were collected.[38] However, the interpretation and application of "necessary" remains ambiguous, raising concerns about the potential improper use of data and the erosion of the rights of privacy of individuals.[39] This ambiguity is particularly worrying in a landscape in which data violations and threats to computer security are increasingly widespread.

The implications of the conservation of indefinite data extend beyond simple privacy concerns; They touch the fundamental human rights sanctioned by the Constitution of Kenya to protect the right to privacy,[40] but adhesion to this right becomes soft when the entities maintain personal data indefinitely, often leading to unauthorized access, theft of identity and profiling. A suggestive example is demonstrated in the legal case of Okiya Omatah[41] The Court highlighted the need for rigorous safeguards and the retention practices of the justified data to protect individual rights The determination of the Court reflected the ongoing tensions between the interest of the state for surveillance and the rights of citizens to privacy.

In practice, the application of the data protection law reveals inconsistencies that undermine its effectiveness. While the law provides for the establishment of the Commissioner's Office for data protection to supervise compliance, this office has faced challenges including limited resources, lack of awareness between the public and insufficient regulatory application mechanisms.[42] The implementation of the law has not been uniform between the sectors, with consequent significant differences in the way the different organizations manage data conservation. Many entities

---

[38] *The Kenya Data Protection Act, (No. 24 of 2019).*

[39] Nyaga B M, Ondego J C, and Joel M, 'Mediation and Data Protection Law in Kenya: Appraising ADR for Optimal Access to Justice under the DPA 2019' Kenya School of Law, 2023, 7 - 40- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4424688 , 20 April, 2023.

[40] Article 31, *Constitution of Kenya,* 2010.

[41] *Okiya Omatah Okoiti v. Attorney General & 2 others*, Petition no. 5 of 2019 eKLR.

[42] Nyaga B 'Mediation and Data Protection Law in Kenya' 25.

continue to archive the data indefinitely, due to the negligence or the lack of understanding of the legal requirements, further complicating the panorama of privacy in Kenya.[43]

In addition, the increase in the digitization of services, in particular in the context of the Covid-19 pandemic, accelerated data collection practices without precise guidelines on the storage timing, increasing the stakes for the privacy protections of the individuals. The cases of law enforcement officers who access data for purposes not outlined in legal doctrines represent further risks, with the potential to establish a surveillance culture that could violate civil freedoms.

As the conversation on data rights evolves, the understanding of the implications of the conservation of indefinite data within the framework of the data protection law becomes an integral part to deal with the concerns of privacy and security. The juxtaposition of legal clauses and practical realities will determine the true effectiveness of this legislation in the protection of people's data rights in Kenya., The 2019 data protection law represents a significant legal structure in Kenya, with the objective of protecting personal data and privacy rights for individuals. Modeled after the European Union's General Data Protection Regulation (GDPR), the law aims to provide a comprehensive legal basis for personal data processing. Central for the law is several important provisions that specifically address data retention, data holders' rights and controllers and data processors obligations.

One of the fundamental aspects of the Data Protection Law is its stipulation during data retention periods. Section 25 of the law requires personal data to be maintained only for the time required for the purposes for which they were processed. This provision highlights the principle of data minimization, which suggests that data controllers should not maintain personal information indefinitely. In addition, since the purpose of data collection ceases, there is an obligation to exclude or anonymize data. This promotes a structure in which the rights of individuals are preserved, as they have the right to erase their personal data ("the right to be forgotten") under specified circumstances.

In addition to stipulating retention periods, the data protection law gives various rights to individuals about their personal data. Notable among these rights are the rights of access,

[43] Nyaga B ‘Mediation and Data Protection Law in Kenya’ 27.

rectification, deletion and restriction of processing. These rights are fundamental to enable individuals to recover the agency on their personal information. Notably, Section 26 allows data holders to request access to their data maintained by any entity, thus creating a mechanism of responsibility and transparency. Such provisions are essential to protect consumer rights as they allow individuals to dispute illegal processing and correcting inaccuracies in their personal data.

However, despite the implementation of these progressive provisions, significant gaps remain in compliance, which impairs the effectiveness of the data protection law in the protection of consumer rights.[44] Many government companies and organizations do not yet have adequate data governance structures, leading to widespread retention of personal data beyond the legally allowed limits.[45] This inconsistent application of data retention practices raises concerns about violating individual privacy rights and misuse of sensitive information.

In addition, the execution mechanisms described in the law are not robust enough. The data Protection Commissioner's office, established to oversee compliance and address complaints, has faced operational challenges, such as limited resources and authority, which make it difficult to comply with their mandate effectively.[46] Consequently, individuals may find it difficult to seek reparation or have their rights maintained in cases of non -compliance. The legal cases that emerged highlight this situation, where individuals fought to affirm their rights against entities that do not adhere to data retention regulations.

In addition, the lack of public awareness of data protection rights exacerbated these problems. Many people may not be fully informed about their rights under the data protection law, leading to a systemic imbalance in power between consumers and service providers.[47] The implications of indefinite data retention, therefore, not only affect the privacy and security of personal information, but also contribute to significant disparities in the protection of consumer rights. These inconsistencies in the application and application of data protection principles require urgent attention to ensure that the desired safeguards for individuals are performed effectively. [48] In short,

---

[44] Nyawara D O, 'Regulation of Fintech: Analysis of data protection provisions aimed at protecting consumers in Kenya' Strathmore University, Thesis, 2021, 34-79, http://hdl.handle.net/11071/12930 , 2021.
[45] Nyawara, D 'Regulation of Fintech' 20.
[46] Nyawara, D 'Regulation of Fintech' 66.
[47] Nyawara, D 'Regulation of Fintech' 66.
[48] Nyawara, D 'Regulation of Fintech' 5.

while the 2019 data protection law provides a promising basis for the protection of personal data in Kenya, gaps in implementation and compliance represent significant challenges to protect consumer rights. Approaching these gaps is crucial to ensuring that the rights of individuals remain in the forefront of data governance practices in the country., The landscape of data retention in Kenya reveals a complex interaction between legal frameworks and judicial interpretations, in particular under the auspices of the 2019 data protection law.

Several significant cases have emerged, highlighting the challenges of the balance of national security and personal confidentiality of data protection principles. One of the key cases is Okiya Omttatah Okoiti the petitioner[49] challenged the legality of government directives requiring telecommunications companies to retain customer data for an extended period. The court ruled in favor of the petitioner, indicating that the general retention of data without clearly defined objectives contravenes the principles of legal processing as adapted to the data protection law. This case is particularly important because it highlights the need for explicit justifications when preserving personal information, defining a precedent for future cases related to data confidentiality.

On the other hand, the case of Julius Karanja[50] provides a more nuanced perspective on the interpretation of data retention laws in the context of law enforcement activities. Karanja challenged police access to his personal data without consent, citing violations of his privacy rights, as protected by the Kenyan Constitution and the Data Protection Act. The court, however, confirmed the actions of the police, interpreting the need to retain data for public security and security as a legitimate interest under the data protection law. This decision illustrates a potential inconsistency in judicial decisions; While protecting individual privacy rights, the courts also recognize the prerogative of the state to maintain personal data in specific circumstances. This balancing law raises questions about the limits of data retention under the data protection law and the legal justification used by the courts.

In addition, the case of Jesse Othoo v. Safaricom[51] highlights the challenges of the application of data protection rights against private entities. Here, Othoo alleged that Safaricom has retained its

[49] *Okiya Omttatah okoiti v Communications Authority of Kenya & 8 Others,* (2018) eKLR.
[50] *Julius Karanja v. National Police Service & 3 Others,* (202)1 eKLR.
[51] *Jesse Othoo v Safaricom Limited,* (2022) eKLR.

data beyond the necessary duration and has failed to give it full access to the information held to it. Although the court has recognized the importance of minimizing data and rights of users under the data protection law, it finally ruled in favor of Safaricom. The decision focused on the idea that data conservation policy was aligned with the company's operational requirements. This case highlights the inconsistency of judicial interpretations concerning the obligations of private entities vis-à-vis the retention of personal data, which suggests that the interests of businesses can sometimes overshadow individual confidentiality.

Another essential aspect to be considered in the discussion of data retention and privacy in Kenya is the role of regulatory organizations such as the office of the Data Protection Commissioner (ODPC). The efficiency and the regulatory framework established by the ODPC have been questioned, in particular concerning the actions of application in light of the aforementioned cases.[52] Many have criticized the inconsistency of the way the ODPC addresses the violations of the public and private sectors concerning data preservation practices.[53] For example, although the ODPC is empowered to study the violations of the data protection law, its approach has been characterized by a lack of proactive measures, allowing various entities to keep data indefinitely without facing significant consequences.[54]

Overall, the fluctuating results of these legal affairs reflect significant ambiguities within the data protection law, in particular concerning the right to privacy and the conditions under which data retention may be justified. The interpretations of the judiciary highlight the urgent need for clearer directives on the retention and use of data, in particular to balance individual rights against increasing data demands by states and businesses. Emerging precedents suggest an in progress critical dialogue on the strict safeguard of personal information, while Kenya continues to combat effective legal frameworks in an increasingly based on data., Undefined retention of data in Kenya has significant risks to individual privacy rights, particularly in a socio-legal context in which the DPA seeks to provide a structure for personal data management and ensure that its processing is performed in a way that respects the dignity of individuals. However, the intersection of the

[52] Mugo E W, 'Governance in the Data Age: Application of Corporate Governance to Ensure Consumer Data Protection in Kenya' University of Nairobi, Thesis, 2018, 22-97 https://erepository.uonbi.ac.ke/handle/11295/108799 , 2018.
[53] Mugo, 'Governance in the Data Age' 38.
[54] Mugo, 'Governance in the Data Age' 44.

provisions of the law and the continuous practice of retaining personal data indefinitely increases critical concerns about privacy and security.[55]

2.4 Impact on Data Privacy and Security

Existential risks associated with prolonged data storage are rooted in various theoretical structures, especially those that defend privacy as a fundamental human right.[56] When personal data are stored for indefinite periods, individuals are subject to a growing probability of privacy violations, particularly in relation to unauthorized access, misuse and potential abuse of third parties, including state actors and not state -owned. This containment resonates with the paradox of privacy, in which the perceived benefits of data sharing and technological integration are overshadowed by the inherent risks of data violations and erosion of privacy.

In the legal scenario of Kenya, several cases exemplify the harmful impact of retention of indefinite data on privacy rights. An example involves the continuous challenges faced by telecommunications companies needed to store user data for a defined period. Notably, the case of Okoth Ochieng[57] stressed the tension between user consent to data processing and the obligation to retain data indefinitely. The court's decision highlighted inconsistencies in how consent is interpreted under the DPA; It has been indicated that many users are usually unaware of their data rights and that consent can be obtained by coercive means rather than an informed contract. This case illustrates not only the legal gaps around consent, but also demonstrates that retention of personal data beyond their need exposes individuals to risks of high privacy.

In addition, the Kenyan government's approach to data retention has often exhibited a challenge of the principles established by DPA. To maintain effective data privacy, there must be a clear distinction between data collection purposes and retention period.[58] Inconsistent practices in data retention in various sectors, such as finance and telecommunications, reveal a systemic failure to incorporate privacy safeguards into organizational policies.[59] Organizations are often involved in

[55] Mugo, 'Governance in the Data Age' 63.
[56] Mugo, 'Governance in the Data Age' 72.
[57] *Okoth Ochieng v Safaricom,* 2021 eKLR.
[58] Mugo, 'Governance in the Data Age' 83.
[59] Mugo, 'Governance in the Data Age' 72.

data retention practices that extend beyond what is necessary for operational purposes, leading to the accumulation of vast sets of data that could inadvertently be misused.[60]

In addition, in the context of national security, the implications of indefinite data retention are even more exacerbated. The Kenyan government usually justifies the extensive collection and retention of data based on improving national security, which raises ethical concerns about the balance between individual privacy rights and state interests. The ambiguity surrounding the legal definitions of national security and the lack of supervision mechanisms to regulate data retention practices expose citizens to possible surveillance and violations in their privacy.

In examining these dynamics, it is evident that the implications of indefinite data retention in Kenya amplify the risks faced by individuals. The intersection of legal inconsistencies, inadequate protection mechanisms and lack of awareness among the population in relation to data rights culminates in an environment where privacy is increasingly compromised. As such, the structure provided by DPA should be analyzed and critically fortified to ensure that personal data protection align with the principles of privacy as an essential human right in Kenya., The emergence of Fintech companies in Kenya represents a significant development in the digital economy of the country, since these entities are increasingly committed to large quantities of data on consumers to provide innovative financial services.[61] The operations of Fintech companies are critically intertwined with the legal paintings established by the 2019 data protection Act (DPA), which aims to regulate data processing activities and protect individuals' privacy. However, the DPA has provisions designed to safeguard the interests of consumers, the practical implications of the retention practices of indefinite data between the Fintech companies raise substantial concerns regarding privacy and security.[62]

Fintech companies, including mobile banking services and payment platforms, collect different data from users, ranging from personal identification information to transactions.[63] Based on the DPA, there are specific provisions that impose that the data must be maintained only for all the

[60] Mugo, 'Governance in the Data Age' 87.
[61] Makulilo A B, 'Privacy in mobile money: Central banks in Africa and their regulatory limits' International *Journal of Law and Information Technology*, 2015, 372–391 - https://doi.org/10.1093/ijlit/eav014 , 25 September 2015.
[62] Makulilo, 'Privacy in mobile money, 372-391.
[63] Makulilo, 'Privacy in mobile money, 372-391.

time necessary to satisfy the purpose for which they were collected. Section 25 of the DPA indicates that data managers must establish a clear retention policy, ensuring that unnecessary data is more safely destroyed. However, reality within the Fintech sector often diverges from these legal clauses. Many companies demonstrate the tendency to keep consumer data indefinitely as a strategic decision to improve customer profiling, the detection of fraud and the customization of the service.[64] This approach, apparently intended to improve the user's experience, raises questions about prevailing practices compared to legal conformity.These cases serve as a reminder that while legislative paintings exist, the implementation and application of these laws remain inconsistent, creating a potential legal emptiness for the Fintech companies operating in Kenya.

In addition, the DPA outlines rigorous conditions for the processing of legitimate data pursuant to section 3, but Fintech companies frequently use large clauses within customer agreements that allow a vast collection and data loyalty.[65] These agreements, often presented in an intricate legal language, can obscure the measure that consumer data will be used, leading to an erosion of informed consent: a fundamental component of data protection.[66] The continuous dependence on vague terms can serve as an escapade that undermines the intention of the DPA, allowing the indefinite conservation of personal data without an adequate awareness or acquiescence of the consumer.

Finally, the mechanisms of liability established by the DPA, including the office of the commissioner for data protection, were slow to mature.[67] The application was limited by factors such as insufficient resources and a lack of technical skills, which further complicates compliance for Fintech companies. Consequently, there is a disparity between legislative ideals and operational realities, potentially exposing consumers to privacy violations and data violations.[68] While the DPA aims to navigate in the growing challenges within the digital economy, the proliferation of indefinite data storage practices raises critical questions about data security and privacy, justifying a revaluation of existing regulatory paintings to adequately deal with these

[64] Makulilo, 'Privacy in mobile money, 372-391.
[65] Makulilo, 'Privacy in mobile money, 372-391.
[66] Makulilo, 'Privacy in mobile money, 372-391.
[67] Oyatsi T R, 'Balancing competing interests: A study on Kenya's Ability to reconcile national security with the right to privacy' Strathmore University, Thesis, 2017 1-51 https://su-plus.strathmore.edu/handle/11071/5590, 2017.
[68] Oyatsi, 'Balancing competing interests' 51.

pervasive issues adequately.[69] In the discourse surrounding data retention policies in Kenya, the argument advances national security as a justification for the indefinite retention of data has become a predominant theme among the government authorities.[70] This argument often positions data retention as a critical mechanism to protect national interests in an increasingly volatile global landscape where threats to security, terrorism and organized crime are perceived as increasing.[71] This justification was used by the State to justify large surveillance measures which infringe the individual rights of privacy and could potentially lead to the abuse of power.

The approval of the indefinite retention of data on the pretext of national security raises significant ethical and legal issues concerning proportionality and the need for these intrusive measures. As articulated in the Data Protection Act (DPA), the limitation of objective requires that personal data should only be collected and kept for specified legitimate purposes. In juxtaposition to this legislative intention, the general application of indefinite retention of data for national security purposes risks undermining the fundamental principles of DPA. A critical examination reveals an inherent tension between the state claim to national security and the protection of individual rights over privacy, leading to an exacerbation of existing inconsistencies in application practices.

The way in which national security is invoked often lacks adequate transparency and monitoring mechanisms, which thus raises concerns about the potential for abusive arbitrary use of the data preserved. Coupled with relatively loose legal frameworks governing data access and sharing, retention without restriction of data constitutes an implicit threat to civil freedoms. For example, the Kenya Police Service has sometimes exploited data to delete dissent and monitor political opposition, situating the argument of national security as a practical cover for potential abuses of authority.

In addition, dependence on national security as a justification for data retention can lead to a frightening effect on free expression and civic commitment. Individuals can hesitate to communicate freely, fearing that their personal communications be monitored under the guise of preventive action against terrorism and crime. This effect is particularly pronounced in contexts

[69] Oyatsi, 'Balancing competing interests' 32.
[70] Oyatsi, 'Balancing competing interests' 33.
[71] Oyatsi, 'Balancing competing interests' 33.

where the legal foundations of such monitoring are insufficiently defined, leading to a perception of omnipresent monitoring and reduced confidence in public institutions.

Several legal affairs that have emerged in this context are used to illustrate the risks associated with indefinite data retention. For example, the case of Kituo Cha Sheria v The Attorney General[72] highlighted the balancing law between national security and individual rights, questioning the validity of the actions of the government which invoke national security without concrete justification. The deliberations of the Court emphasized the need for a clear legal framework which delimits the circumstances in which the data can be accessible or kept for national security purposes, thus stressing the need for responsibility in the management of personal data.

On the other hand, the private sector demonstrates a more diverse approach to data retention, influenced by the nature of industry and the resources of entities. Some organizations, such as telecommunications providers and financial services, tend to retain customer data for prolonged periods due to regulatory requirements and the need for business continuity.[73] For example, the Kenya Communications Authority requires telecommunications companies to maintain call records for a minimum of two years to support investigations of law application.[74] However, this practice raises ethical questions about the balance between public security and individual privacy rights. Companies usually do not have robust data governance structures to track these requirements, resulting in prolonged retention periods that do not align with the principles described in DPA.[75]

In addition, sectors such as health exhibit remarkable inconsistencies in adherence to DPA. Health service providers often maintain patient records indefinitely - an essential practice to ensure continuity of care. However, many institutions do not establish transparent data retention policies that inform patients about how their data will be used and retained. This inconsistency can lead to violations of confidentiality and mine public trust in health systems.

---

[72] *Kituo Cha Sheria & 8 others v The Attorney General,* (2013) eKLR.
[73] Maseh E, 'Managing court records in Kenya' 25 *African Journal of Library,* Archives & Information Science, 2015, 155- 171.
[74] Maseh, 'Managing court records in Kenya'
[75] Maseh, 'Managing court records in Kenya'

Non -compliance with data retention policies introduces a spectrum of consequences in these sectors. Legal penalties, including fines and sanction orders issued by the ODPC, are criticism in catalyzing adherence to data protection laws. However, the execution process may be inconsistent, usually dependent on the sector and resources available for regulatory supervision. In addition, the absence of an intersectoral approach consistent with data governance exacerbates the problem, as sectors can adopt varied interpretations of the law, leading to a fragmented regulatory landscape.

In short, discrepancies in data retention practices in the public and private sectors of Kenya illustrate a pressing need for unified standards and compliance mechanisms that align with the ideals of the Data Protection Law. Approaching these inconsistencies is essential not only to protect individual privacy rights, but also to improve the general data security and public trust in data management practices. Thus, continuous involvement with stakeholders, together with monitoring and rigorous assessment of data retention protocols, is imperative to reinforce the integrity of the data protection structure in Kenya., International data protection regulations provide a reference to evaluate national structures, including the Kenyan Data Protection Law (DPA) promulgated in 2019. By examining the implications of these regulations, we can discover systemic issues in Kenyan practices related to retention of undefined data and how these questions renounce global standards.

Notably, inconsistency in practices around data retention in Kenya is amplified by the absence of clear guidelines and DPA application mechanisms. For example, although the law ostensibly promotes the protection of personal data, there were cases of extended illegal retention of data by government agencies and private entities without justification. This contradicts the data protection principles established in international structures, leading to systemic issues in compliance and implementation. The situation is even more complicated by the fact that several administrative agencies operate with limited supervision and lack adequate training in data protection, as highlighted in Njoya v. The Attorney General (2021)[76], where a citizen's data were retained without proper legal grounding.

In addition, comparisons with structures such as the California Consumer Privacy Law (CCPA) reveal additional deficiencies in the Qenia regulatory scenario. CCPA emphasizes consumer rights

[76] *Rev Dr Timothy M Njoya & 6 others v The Hon Attorney General & 4 others*, (2004) eKLR.

regarding access to data, exclusion and right to the option of selling data, promoting transparency and user control. Although DPA identifies the right to access personal data, provision for an explicit option mechanism is absent, limiting individuals' ability to affirm control over their information. The implications of this deficiency are deep, particularly in undermining the effectiveness of DPA in protecting user privacy.

In addition, divergent international standards on data location expose additional vulnerabilities in the Kenyan context. Compliance with data location mandates, as practiced in regions such as Asia and Europe, could improve the security of personal data. However, Kenyan entities usually fail to adapt to these international standards, given the general challenges related to data storage infrastructure and the lack of consistent regulatory supervision.

Individuals face difficulties in search of reparation when their data rights are violated, especially when institutions do not align their practices with regulatory standards. This detachment between legislation and practice highlights a critical gap in Kenya's data protection structure, in which the law exists, but lacks the necessary institutional support for effective implementation.

The implications of retention of indefinite data in Kenya, as governed by the data protection law, are multifaceted and complex, raising critical concerns about privacy, security and legal responsibility.[77] The interaction between legislative intent and practice of the real world reveals inconsistencies that can undermine the very objectives of the Data Protection Law.[78] Although the law has been created to provide a structure for personal data protection, the absence of rigorous guidelines on the duration of data retention and the conditions under which data can be stored significantly.[79]

The case of Anyang 'nyong'o[80] highlighted tensions between government data retention strategies and constitutional law to privacy. In this case, the Supreme Court found that the indiscriminate practices of data retention of state agencies collected from the fundamental rights of citizens,

---

[77] Ayalew Y E, 'Untrodden paths towards the right to privacy in the digital era' *International Data Privacy Law,* 2022, 2-41 - https://doi.org/10.1093/idpl/ipab031, 2022.
[78] Medi M, 'Online Surveillance and Freedom of Expression in Kenya' University of Nairobi, Thesis, 2021, - http://erepository.uonbi.ac.ke/handle/11295/161037, 2021.
[79] Medi, Medika 'Online Surveillance and Freedom of Expression in Kenya' 39.
[80] *Prof Peter Anyang' Nyong'o and Others vs Attorney General of Kenya and Others* (2019) eKLR.

reinforcing the statement that these practices must adhere to the established legal structures that prioritize individual privacy. These judicial findings reveal a pressing need for a reassessment of current data retention practices that lack clear limitations and safeguards for personal data.

In addition, inconsistency in practices between different - public and private entities - covers the urgent need for generalized compliance and regulation. In some cases, organizations have claimed adherence to data protection principles, but usually fail to implement robust data governance structures. Factors such as organizational culture, digital division and technological capabilities have resulted in a disparate understanding of how to protect personal information. This inconsistency not only compromises the individual privacy of citizens, but also culminates in possible safety vulnerabilities that can be explored by cybercriminals.

The social implications of indefinite data retention cannot be neglected. Retention of personal data without sufficient reason creates a risk of misuse and stigmatization of individuals, disproportionately affecting disadvantaged groups.[81] Data holders may be vulnerable to discrimination due to decisions based on their retained data - decisions that may not accurately reflect their current circumstances or behavior. A humiliating aspect of data retention is its potential to perpetuate systemic inequalities, ensuring rigorous discourse and action to align practices with the principles of justice.[82]

As Kenya advances in its digital transformation, the potential risks associated with indefinite data retention require a balanced approach that respects privacy, allowing the use of beneficial data. The search for innovation should not overshadow the call for responsible data management. Establishment of clear retention periods, informed consent processes, and enhanced mechanisms for data governance would significantly mitigate the inherent risks associated with data retention. Legal structures must be harmonized with operational practices, ensuring responsibility at individual and organizational levels, thus promoting an environment in which privacy rights are maintained and security is maintained.

In short, the complexities around the retention of indefinite data under the Kenyan Data Protection Law point to an urgent need for reform. The legal scenario should evolve to promote consistent

[81] Ayalew Y 'Untrodden paths towards the right to privacy in the digital era,'10.
[82] Ayalew Y 'Untrodden paths towards the right to privacy in the digital era,' 40.

practices that protect individual privacy and security, addressing the multiple interests present in society. A united effort that incorporates voices of stakeholders - government, civil society and private sector - will be critical to achieving a more equitable and secure data environment for all Kenyans.

Indefinite data retention poses significant risks to data privacy and security. When organizations retain data for longer than necessary, they increase the likelihood of unauthorized access and data breaches.[83] This can lead to severe consequences for both individuals and organizations.

Indefinite data retention increases the volume of data that needs to be protected, making it more challenging to secure.[84] The larger the data set, the more attractive it becomes to cybercriminals.[85] For individuals, data breaches can result in identity theft, financial fraud, and other malicious activities.[86] The exposure of personal information can have long-lasting effects on an individual's financial and personal life.[87] For organizations, the consequences can be even more severe. Data breaches can lead to financial losses, damage to reputation, and legal liabilities.[88] The cost of a data breach can be substantial, with the average cost reaching millions of dollars.[89]

Under the Kenya Data Protection Act, organizations are required to implement appropriate measures to protect personal data, and failure to do so can attract hefty penalties.[90] Furthermore, the long-term retention of data without clear guidelines can complicate data governance, making it challenging for organizations to maintain data accuracy and integrity. This can hinder decision-

[83] Connolly L, Wall D S, Lang M, and Oddson B, 'An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability' *Journal of Cybersecurity,* 2020 - https://doi.org/10.1093/cybsec/tyaa009, 2020.
[84] Connolly L, 'An Empirical Study of Ransomware Attacks on Organizations' 11.
[85] Connolly L, 'An Empirical Study of Ransomware Attacks on Organizations' 12.
[86] Kitili J and Abiero D, 'Kenya's Digital Infrastructure Under Threat; A Look at Anonymous Sudan's Thwarted Cyber Attack Attempt and its Implications for Kenya's Digital Systems' *Centre for Intellectual Property and Information Technology Law*, 2023, https://cipit.strathmore.edu/kenyas-digital-infrastructure-under-threat-a-look-at-anonymous-sudans-thwarted-cyber-attack-attempt-and-its-implications-for-kenyas-digital-systems/, August 2023.
[87] Kitili J, 'Kenya's Digital Infrastructure Under Threat'
[88] Kitili J and Abiero D, 'Kenya's Digital Infrastructure Under Threat'
[89] Harris S, *Cybersecurity: A Comprehensive Guide to Information Security*, *McGraw-Hill Education*, New York, 2015.
[90] Greenleaf G, Data Protection and Privacy: A Global Perspective, 2nd Edition, Springer, Singapore, 2017.

making processes, as outdated or irrelevant data may be inadvertently used, impacting the quality of business insights and strategies.[91]

2.5 Conclusion

In summary, the Kenya Data Protection Act provides a fundamental framework for managing data retention within the country. However, the ambiguity surrounding the interpretation of "reasonable and necessary" in Section 39 presents significant challenges for Data Controllers and Data Processors. The lack of explicit guidelines leads to inconsistent practices, which can result in prolonged data retention, increased risks of unauthorized access, data misuse, and breaches. Moreover, these risks have far-reaching consequences, not only affecting individuals' privacy and security but also impacting organizations' compliance, reputation, and overall data governance.

To mitigate these risks, it is crucial for organizations to develop clear data retention policies ensuring that personal data is retained only for as long as necessary. This involves balancing the need for operational, legal, and regulatory compliance with the imperative to protect individuals' privacy and security. Having examined the legal framework and the challenges posed by indefinite data retention under the Kenya Data Protection Act, the next chapter will delve into how Data Controllers and Data Processors interpret the terms "reasonable" and "necessary."

CHAPTER 3

INTERPRETING “REASONABLE AND NECESSARY” IN GERMAN DATA RETENTION PRACTICES

3.1 Introduction

In this chapter, we will analyze the interpretation of "reasonable" and "necessary" in the context of Germany's data retention practices. This involves examining how German data controllers and processors balance the need to retain personal data for operational, legal, and regulatory purposes with the imperative to protect individuals' privacy and security. Germany's jurisdictional

[91] Harris S, *Cybersecurity: A Comprehensive Guide to Information Security*, 2015.

framework, shaped by both national and EU legal developments, provides a critical backdrop for this analysis. The country's history with data retention laws, including the invalidation of previous legislation by the Federal Constitutional Court and the European Court of Justice's rulings on EU directives, highlights the challenges in defining what is "reasonable" and "necessary" in data retention.

The objective of this chapter is to understand how German organizations navigate these legal complexities to ensure compliance with data protection regulations while retaining data for legitimate purposes. By examining Germany's specific legal frameworks, such as the Telecommunications Act (TKG) and recent ECJ judgments, we will explore how different approaches to data retention impact organizational efficiency, data privacy, and compliance. This analysis will provide insights into the challenges faced by German data controllers and processors in managing data retention responsibly, particularly in light of the EU's emphasis on proportionality and privacy rights. Through this exploration, we aim to shed light on best practices and potential reforms that could enhance the balance between data retention needs and privacy protections in Germany.

3.2 Balancing Privacy and Security: The Principle of "Reasonable and Necessary" in Data Retention Laws

3.2.1 Judicial Precedent in Germany.

The principle of "reasonable and necessary" in data retention laws requires that any data retention measures must be proportionate to the legitimate aim pursued, such as combating serious crime, and must not exceed what is necessary to achieve that aim. Digital Rights Ireland v Ireland,[92] The Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive, ruling that it disproportionately interfered with fundamental rights to privacy and data protection.[93] The case challenged the legality of the EU Data Retention Directive, which required telecommunications data to be retained for law enforcement purposes. The plaintiff argued that this directive violated privacy and data protection rights such as the right to respect for private and

[92] *Digital Rights Ireland Ltd. v. Ireland,* (2014) The European Court of Justice.
[93] *Digital Rights Ireland Ltd. v. Ireland,* (2014) The European Court of Justice.

family life,[94] right to protection of personal data[95] and the right to respect for private and family life.[96] The CJEU declared the Data Retention Directive null and void, citing severe interference with privacy and data protection rights.[97] Courts argued that data retention laws excessively interfered with individuals' privacy and personal data protection rights. The measures were deemed disproportionate to their intended purpose of combating serious crime, as they involved mass surveillance of all citizens. Courts highlighted the lack of adequate legal safeguards to ensure that only authorized individuals could access retained data.

The court's interpretation of reasonable and necessary data retention practices focused on balancing privacy rights with security needs. The court scrutinized whether the retention period and the scope of data collected were proportionate to the intended purpose of combating serious crime.[98] It emphasized that data retention should not be excessive and must be subject to strict oversight to prevent abuse. The court also highlighted the importance of independent supervision and clear, precise regulations to ensure that data access is limited to what is strictly necessary for specific, legitimate purposes, thereby protecting individuals' privacy rights while addressing security concerns.

In another case, Tele2 Sverige AB v. Post- och telestyrelsen, involved Tom Watson, Peter Brice, and Geoffrey Lewis challenging the Data Retention and Investigatory Powers Act 2014 (DRIPA),[99] which mandated data retention by a Swedish telecommunications provider, it ceased retaining electronic communications data following the Digital Rights Ireland decision, which invalidated the EU Data Retention Directive[100] due to its incompatibility with fundamental rights. The CJEU ruled that EU law precludes national legislation that imposes a general and indiscriminate retention of data. Such measures were deemed incompatible with the fundamental

[94] Article 7, *Charter of Fundamental Rights of the European Union* (2010).
[95] Article 8, *Charter of Fundamental Rights of the European Union (2010).*
[96] Article 8 *European Convention on Human Rights* (2007).
[97] *Digital Rights Ireland Ltd. v. Ireland,* (2014) The European Court of Justice.
[98] Podkowik J, Rybski R, and Zubik M, 'Judicial dialogue on data retention laws: A breakthrough for European constitutional courts' *International Journal of Constitutional Law*, 2021, 1597-1631 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4637947 , 2021.
[99] *Tele2 Sverige AB v. Post- och telestyrelsen,* 2014, The European Court of Justice (ECJ).
[100] *Directive 2006/24/EC European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*, 2006.

rights to respect for private life and the protection of personal data[101] (Articles 7 and 8 of the Charter of Fundamental Rights of the EU). The Court allowed for targeted data retention, but only under strict conditions.[102] Retention must be limited to what is strictly necessary and aimed solely at fighting serious crime. It must be proportionate, considering the categories of data retained, the means of communication affected, the persons concerned, and the duration of retention.[103] The CJEU's rationale was grounded in the need to balance national security interests with the protection of fundamental rights. The Court emphasized that any interference with the rights to privacy and data protection must be strictly necessary and proportionate. The judgment reinforced the importance of safeguarding personal data and ensuring that any data retention measures are justified and limited to what is essential for combating serious crime.[104]

The judicial dialogue on data retention laws in Europe has been significantly shaped by interactions between national constitutional courts, the Court of Justice of the European Union (CJEU), and the European Court of Human Rights (ECtHR).[105] This dialogue has been crucial in developing a coherent approach to data retention that balances national security interests with fundamental rights to privacy and data protection. This mechanism ensures uniform application of EU law across states and allows national courts to seek guidance on complex legal issues. Courts engage in comparative analysis of judgments from other jurisdictions to inform their own decisions. This practice helps in identifying common principles and standards, fostering a more harmonized approach to data protection.

Germany's approach to data retention has been influenced by its strong constitutional protections for privacy and data protection. The Federal Constitutional Court (Bundesverfassungsgericht) has played a key role in scrutinizing data retention laws to ensure they comply with fundamental rights.[106] German courts emphasize that data retention measures must be proportionate and

[101] *Tele2 Sverige AB v. Post- och telestyrelsen*, 2014, The European Court of Justice (ECJ).
[102] Podkowik J,'Judicial dialogue on data retention laws' 1620.
[103] Jan Podkowik,'Judicial dialogue on data retention laws' 1598.
[104] Jan Podkowik,'Judicial dialogue on data retention laws' 1609.
[105] Jan Podkowik,'Judicial dialogue on data retention laws' 1597.
[106] Jan Podkowik,'Judicial dialogue on data retention laws' 1607.

necessary. This means that any interference with privacy must be justified by a legitimate aim and must be the least intrusive means available.[107]

The case of Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH, decided by the Grand Chamber of the Court of Justice of the European Union (CJEU) on September 20, 2022.[108] This case involved a request for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Germany). The case arose from the German Federal Administrative Court's referral regarding the interpretation of the Telecommunications Act (TKG), specifically the retention periods for traffic and location data. SpaceNet AG and Telekom Deutschland GmbH, telecommunications service providers, were required to retain such data for specific periods: 4 weeks for location data and 10 weeks for traffic data. The main issues in this case were; Whether the retention periods set by the TKG were compatible with EU law, particularly Directive 2002/58/EC (the ePrivacy Directive) and whether the retention periods set by the TKG balance between national security interests and the protection of fundamental rights, such as privacy and data protection.

The CJEU emphasized the principles of proportionality and necessity in data retention. The Court ruled that general and indiscriminate retention of traffic and location data is incompatible with the fundamental rights to respect for private life and the protection of personal data (Articles 7 and 8 of the Charter of Fundamental Rights of the EU).[109] The Court allowed for targeted data retention but only under strict conditions, ensuring that retention is strictly necessary and proportionate to the aim pursued.[110] The judgment reinforced the importance of safeguarding personal data and ensuring that any data retention measures are justified and limited to what is essential for combating serious crime.[111] The Court highlighted the need for clear, precise regulations and independent supervision to prevent abuse and protect individuals' privacy rights. This case is significant as it clarifies the legal framework for data retention in the EU, emphasizing the balance between security needs and fundamental rights

[107] Jan Podkowik,'Judicial dialogue on data retention laws' 1629.
[108] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*, (2022).
[109] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH,* 2022.
[110] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH,* 2022.
[111] *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*, 2022.

Germany has a comprehensive data retention framework governed by the Federal Data Protection Act (BDSG) and the Telecommunications Act (TKG). The Federal Constitutional Court (FCC) has played a significant role in shaping these laws for example EU Data Retention Directive (DRD),[112] Implemented in Germany, was later declared unconstitutional by the FCC in 2010. It also ensures that telecommunications data must be retained for 10 weeks, and location data for 4 weeks. The European Court of Justice (ECJ) ruled that the German data retention laws were incompatible with EU law, emphasizing the need for targeted data retention. Data retention laws have been a contentious issue, particularly in light of EU regulations and court rulings.[113] The principal data protection legislation is the General Data Protection Regulation (GDPR), supplemented by the Federal Data Protection Act (BDSG). Specific regulations for telecommunications are outlined in the Telecommunications Act (TKG) and the Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG). Here, telecommunications service providers are required to store location data for four weeks and traffic data for ten weeks and this data must be made available to law enforcement authorities upon request.[114]

The Court of Justice of the European Union (CJEU) has repeatedly clarified that general obligations to retain data exceed what is necessary in a democratic society.[115] The balance between national security needs and the protection of fundamental rights, highlights the tension between ensuring security and safeguarding privacy. It also explores the varying interpretations and implementations of data retention laws by different member states, reflecting the ongoing debate over the legitimacy and scope of such measures. Key judgments by the CJEU, such as the Digital Rights Ireland and Tele2 Sverige cases, which have significantly influenced the legal landscape of data retention in the EU. These rulings emphasize the need for proportionality and necessity in data retention measures,[116] asserting that indiscriminate data collection violates fundamental rights. Challenges posed by national security exceptions and the differing stances of national

[112] Rojszczak M, 'National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts' *European Constitutional Law Review,* 2021, 607-635, https://doi.org/10.1017/S1574019621000353 , 2021.
[113] Rojszczak M, 'National Security and Retention of Telecommunications Data' 630
[114] *Telecommunications Act (TKG).*
[115] Rojszczak M, 'National Security and Retention of Telecommunications Data' 612.
[116] Rojszczak M, 'National Security and Retention of Telecommunications Data' 612

courts, such as the Conseil d'Etat in France, which sometimes conflict with the CJEU's standards.[117]

3.2.2 Judicial precedent in Kenya

Kenya has collected extensive biometric data without adequate safeguards, posing significant privacy risks. In the case *Nubian Rights Forum and Others v. The Hon. Attorney-General and Others (eklr)*[118] involved a legal challenge against amendments made to the Registration of Persons Act through the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018, on whether the amendments established the National Integrated Identity Management System (NIIMS), which aimed to create a single repository of personal information for all Kenyan citizens and registered foreigners was constitutional.

The petitioners, including the Nubian Rights Forum, the Kenya Human Rights Commission, and the Kenya National Commission on Human Rights, argued that the amendments were unconstitutional as they violated the right to privacy and posed serious threats to fundamental rights and freedoms. They also claimed that the amendments were passed without adequate public participation and in bad faith.[119]

The High Court of Kenya ruled in favor of the petitioners, declaring that the collection of DNA and GPS data under the NIIMS was an unjustifiable infringement of the right to privacy and therefore unconstitutional. The court also held that the general data protection framework was insufficient and that the entire system could only be implemented after a comprehensive data protection regulatory framework was adopted.[120] This case highlights the importance of robust data protection laws and the need for adequate safeguards to protect individuals' privacy rights in the digital age. The High Court in Kenya declared the rollout of biometric Huduma cards under the National Integrated Identity Management System (NIIMS) unconstitutional. The court ruled that the Data Protection Act of 2019 should be applied retroactively to the government's rollout of NIIMS, which began in November 20202. The decision emphasizes the importance of privacy and

[117] Rojszczak M, 'National Security and Retention of Telecommunications Data' 618.
[118] *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Soc.iety & 8 others* eKLR.
[119] *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others* eKLR.
[120] *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others* eKLR.

data protection, highlighting that the government should have ensured a legal framework for protecting the right to privacy before implementing the system. The ruling mandates a data protection impact assessment before processing data in the system.

In another case involving a complaint filed by the law firm Wamae & Allen Advocates against its former employees, Florence Mathenge and Ambrose Waigwa.[121] The former employees allegedly shared confidential information, including court documents and client data, without consent.[122] This raises concerns about how long such data should be retained and who has access to it. The law firm, as a data controller, failed to report the breach to the Office of the Data Protection Commissioner (ODPC) within the required 72 hours, indicating lapses in data retention policies and breach notification procedures.[123] Many of the documents shared were already public records, which complicates the issue of data retention since public records are not subject to the same retention rules as private data.[124]

Another case involved a claim by Jessica Clarise Wanjiru against Davinci Aesthetics & Reconstruction Centre for the unauthorized use of her image.[125] In July 2016, Davinci Aesthetics & Reconstruction Centre used Jessica Clarise Wanjiru's image in billboards advertising reconstruction and plastic surgery services without her consent.[126] Jessica Clarise Wanjiru argued that this unauthorized use violated her personality rights, specifically her right to control the commercial use of her image. The High Court ruled in favor of Jessica Clarise Wanjiru, emphasizing the importance of obtaining consent before using someone's image for commercial purposes.[127] The petitioner claimed that her personal data, including images, was retained and used without her consent, violating her privacy rights under the Kenyan Constitution.[128] The case highlighted the need for clear guidelines on data retention and the interpretation of "reasonable

[121] *ODPC Complaint No 677* (2022), Office of the Data Protection Commissioner.
[122] *ODPC Complaint No 677* (2022), Office of the Data Protection Commissioner.
[123] *ODPC Complaint No 677* (2022), Office of the Data Protection Commissioner.
[124] *ODPC Complaint No 677* (2022), Office of the Data Protection Commissioner.
[125] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government* (2017) eKLR
[126] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government* (2017) eKLR
[127] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government* (2017) eKLR
[128] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government* (2017) eKLR

and necessary" under the Kenya Data Protection Act. The court emphasized the importance of explicit consent for data retention and usage, setting a precedent for how personal data should be handled by organizations.[129]

3.3 Comparison of Data Retention in Germany and Kenya

In Germany, The Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive, ruling that it disproportionately interfered with fundamental rights to privacy and data protection.[130] The case challenged the legality of the EU Data Retention Directive, which required telecommunications data to be retained for law enforcement purposes. The CJEU declared the Data Retention Directive null and void, citing severe interference with privacy and data protection rights. Courts argued that data retention laws excessively interfered with individuals' privacy and personal data protection rights due to mass surveillance without adequate legal safeguards. another case challenged to the Data Retention and Investigatory Powers Act 2014 (DRIPA) by Tom Watson, Peter Brice, and Geoffrey Lewis.[131] The CJEU ruled that EU law precludes national legislation that imposes a general and indiscriminate retention of traffic and location data, deeming such measures incompatible with the fundamental rights to respect for private life and the protection of personal data (Articles 7 and 8 of the Charter of Fundamental Rights of the EU). The Court allowed for targeted data retention but only under strict conditions, ensuring that retention is strictly necessary and proportionate.

The Federal Constitutional Court (Bundesverfassungsgericht) in Germany has emphasized that data retention measures must be proportionate and necessary. Any interference with privacy must be justified by a legitimate aim and must be the least intrusive means available. This judicial dialogue has been crucial in developing a coherent approach to data retention that balances national security interests with fundamental rights to privacy and data protection.

In Kenya, the judiciary has addressed data retention primarily through the lens of privacy rights and the adequacy of safeguards in place to protect personal data. Nubian Rights Forum,[132] involved

---

[129] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government* (2017) eKLR

[130] *Digital Rights Ireland Ltd v Ireland* (2014), The European Court of Justice.

[131] *Tele2 Sverige AB v Post- och telestyrelsen,* (2014), The European Court of Justice.

[132] *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others* eKLR.

a legal challenge against amendments made to the Registration of Persons Act through the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018. The amendments established the National Integrated Identity Management System (NIIMS), creating a single repository of personal information for all Kenyan citizens and registered foreigners. The High Court ruled in favor of the petitioners, declaring that the collection of DNA and GPS data under NIIMS was an unjustifiable infringement of the right to privacy and therefore unconstitutional. The court held that the general data protection framework was insufficient and mandated a comprehensive data protection regulatory framework before implementing such a system. Another case involved a complaint filed by a law firm against its former employees for allegedly sharing confidential information without consent. The case highlighted concerns about data retention policies, breach notification procedures, and the need for clear guidelines on data retention.[133] The other case involved the unauthorized use of the petitioner's image by a commercial entity without her consent.[134] The High Court ruled in favor of Jessica Clarise Wanjiru, emphasizing the need for explicit consent for data retention and usage under the Kenya Data Protection Act.

The focus on proportionality and necessity ensures that data retention measures are justified by legitimate aims, such as combating serious crime, and are the least intrusive means available. The Federal Constitutional Court, influenced by the CJEU and the European Court of Human Rights, plays a crucial role in scrutinizing data retention laws to ensure compliance with fundamental rights.[135] In Kenya, the emphasis is on safeguarding privacy rights and establishing adequate legal frameworks before implementing data retention systems. The High Court has ruled against initiatives lacking sufficient privacy safeguards, highlighting the need for robust data protection laws and comprehensive regulatory frameworks. Cases such as Nubian Rights Forum and Jessica Clarise Wanjiru underscore the importance of explicit consent and proper data protection measures. There is a critical need for clear and unambiguous frameworks on data retention periods in Kenya. Such frameworks should ensure that data retention measures are strictly necessary, proportionate, and include explicit guidelines on retention periods to protect privacy rights and enhance compliance with data protection laws.

---

[133] *ODPC Complaint No 677,* 2022, Office of the Data Protection Commissioner.

[134] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre, Nang'ole Wanjala & Nairobi City County Government* (2017)

[135] Jan Podkowik,'Judicial dialogue on data retention laws' 1629.

The 2019 Data Protection Act (DPA 2019) represents crucial progress in the legal landscape governing data protection in several jurisdictions, establishing complete directives which aim to regulate the activities of data controllers and processors. Mainly, DPA 2019 establishes a framework for legal processing of personal data, demanding that all data preservation practices align with fundamental principles of necessity and reasonable nature. These principles serve as pivotal siders to determine the authorized scope and duration of data retention, thus guiding both the ethical and legal frameworks in which the organizations operate.

The concept of "necessity", as articulated within the 2019 DPA, obliges data controllers and processors to verify that any retention of personal data is strictly essential to achieve the specified objectives for which the data has been collected. This imperative to adhere to the need is rooted in the broader ethics of DPA, which seeks to limit the processing of data to the minimum required to achieve legitimate objectives. For example, under specific circumstances, a data preservation period may be justified if it directly concerns a commercial function or a particular legal obligation, such as compliance with tax regulations or other legal requirements. The presumption here is clear; Organizations must engage in risk assessments and carefully assess whether the retention of special data sets is essential for operational continuity or regulatory compliance.

Concomitantly, the concept of "reason" plays an additional role within the DPA 2019. Although the need focuses on the absence of alternatives, the reasonable nature assesses proportionality and is justified to keep data concerning the objectives for which is treated. It serves as a measure to assess whether retention practices have found an appropriate balance between the interests of the organization and the rights to the confidentiality of individuals. The incorporation of reasonable nature in the legislative framework guarantees that data preservation measures do not exceed what is justified from the point of view of companies and that the hoarding of excessive or unjustified data is discouraged.

The 2019 DPA underlines the need for a dynamic approach to data retention, requiring regular journals of data sets preserved to determine their relevance and their continuous necessity. This current assessment facilitates not only adherence to the principles of necessity and reasonable character, but also reflects the culture of the compliance of an organization, demonstrating a commitment to protect individual privacy in an evolving data landscape. In addition, organizations

are encouraged to develop clear internal policies that elucidate their data retention strategies, supported by solid data governance practices aligned with the principles set out in the law.

It is essential to recognize the practical implications of this legislative framework for data controllers and processors. The requirement of a balance between data protection and commercial imperatives promotes an environment where organizations can operate effectively while minimizing the risk of non-compliance. This balance becomes particularly salient when browsing the competitive commercial landscape, where data -based ideas can considerably improve operational efficiency and consumer commitment. However, DPA 2019 also obliges a cautious approach, convincing organizations to contemplate the ramifications of in -depth retention of data not only in terms of regulatory risk, but also concerning the consequences of reputation resulting from data violations or use of potential data.

Given the 2019 DPA shades, there is a palpable need for organizations to actively integrate these legal principles into their data management practices. In doing so, data controllers and processors can better navigate the tension between operational requests and the imperative to respect and protect individual confidentiality rights, ultimately guiding their data conservation practices in a responsible framework and enforceable in accordance with legislation.[136] The concept of necessity is a central criterion under the DPA. The DPA stresses that personal data can only be kept if such retention is necessary to achieve specific objectives, as well as delimited in legislation.[137] More specifically, the need emerges during data processing steps, in which data and data processors are mandated to demonstrate that their data storage practices are aligned with legal obligations, contractual requirements or the realization of legitimate interest which is not exceeded by the rights of data subjects.[138] The explicit requirement of necessity is used to alleviate the risks of excessive data retention, to align with the principles of proportionality and responsibility.

In particular the DPA 2019 claims that data retention will be considered necessary when it is essential for the application of Common Law or statutory obligations.[139] Such a requirement

---

[136] Wachter S and Mittelstadt B, 'A right to reasonable inferences: re-thinking data protection law in the age of big data AI' *Columbia Business Law Review*, 2019, 2- 130 https://journals.library.columbia.edu/index.php/CBLR/article/view/1234 , published 2019.
[137] Wachter S and Mittelstadt B, 'A right to reasonable inferences' 50.
[138] *Data Protection Act,* 2019.
[139] Section 3, *Data Protection Act,* 2019.

requires that the data controller or the processor performs a deliberate evaluation to determine that the retention period must not exceed what is necessary to satisfy the specific objective. Several thresholds are established within the DPA, including the duration for which the data is kept being proportionate to the objective, the legitimacy of the interests pursued and the impact on the rights and freedoms of data subjects. This necessity -based approach encourages a solid assessment framework which must be periodically revised to ensure compliance.

During a comparative analysis with German law, which is articulated in the Federal Data Protection Act (BDSG), the interpretation of the need has notable similarities and notable differences. German law adheres to a similar basis by establishing that data processing, including retention, should only occur when it is necessary for the purposes defined under the General Data Protection Regulations (RGPD) or other relevant legal provisions. However, German interpretation emphasizes the socio-legal context in which data processors operate, causing an influence of the country's historical experiences with data confidentiality.

The Federal Data Protection Authority German marks a strict approach to data retention policies, accentuating strict adhesion to the principle of data minimization as devoted to the GDPR.[140] This affects the way in which the need is interpreted, in particular concerning public and private interests, by which an assessment of broader societal value can come into play. The case law of the German courts has strengthened this notion, establishing precedents where judges have ratified the assertion that retention practices should only occur within closely defined limits which are manifestly justified. For example, in the historic case of the Federal Constitutional Court of Germany,[141] The Court affirmed that data conservation practices could only be justified in case the data controllers articulate a strong justification for prolonged retention.

In addition, the interaction between German and European case law underlines how interpretations of the need can lead to periods of detention of various data between the courts. In an increasingly interconnected European environment, the German courts have influenced European directives for the protection of European data, promoting a strict perspective on the retention of data which could impose more strict considerations than those which prevail under DPA 2019 . Such interpretations

[140] Article 5, *General Data Protection Regulation*, (GDPR)
[141] *Bundesverfassungsgericht, NJW 822*, 2008.

require organizations operating in several jurisdictions to assess their frameworks of conformity carefully, ensuring that their data preservation policies align not only on national regulations, but also in accordance with increased standards established by previous cases. Consequently, this comparative analysis illustrates a fundamental divergence in the way in which the need is perceived and operationalized in data retention policies, highlighting the potential ramifications for data controllers navigating these legal paradigms., When analyzing the concept of "reasonableness" within the data retention framework under the Data Protection Act, and the German law, it is imperative to delineate how these legal paradigms operationalize the expected standards of data controllers and processors . Both legal frameworks emphasize the principle of data minimization, ensuring that personal data is kept only as necessary for the aims for which it was collected. However, the interpretation and application of "reasonableness" manifest different patterns in each jurisdiction.

The 2019 DPA incorporates the concept of reasonableness by stipulating that data retention practices should be aligned with the identified purpose of data processing. This is closely aligned with the definitions encapsulated in the European General Data Protection Regulation (GDPR), which underlines the need for clarity in the retention periods. The reasonableness standard requires data controllers and processors to participate in a contextual analysis, balancing the operational needs against people's privacy rights. It is established that the retention must not only be necessary but also in line with the relevance of the data for the purpose carried out.[142] A failure to meet these criteria can lead to possible responsibilities.

In practice, the reasonableness standard has been illuminated through several notable jurisprudence developments. For example, the case of Google LLC v. CNIL [143] In the context of the GDPR interrogates the scope of data retention practices, emphasizing that although data controllers have certain degrees of operational discretion, this discretion is not absolute. The Court ruled that the provisions governing data withholding must comply with a criterion of clear necessity, which implicitly reinforces a reasonableness standard.

[142] Section 18, *Data Protection Act*, 2019.
[143] *Google LLC v CNIL, C-507/17,* The European Court of Justice (ECJ)

On the contrary, the German Data Protection Law, governed mainly by the Federal Data Protection Law (BDSG), defends an equally rigorous position regarding reasonableness. However, it diverges in its application through greater administrative granularity and an established framework of coded principles within the BDSG and the relevant jurisprudence. According to the Federal Data Protection Law, the data must be eliminated as soon as retention purposes are fulfilled unless otherwise specified by legal regulations.[144] This requires that data controllers not only evaluate the practicality of data retention, but also rigorously justify the retention period through transparent metrics of commercial needs.

The German courts have also clarified the principle of reasonableness in emblematic decisions, such as R. (in the Black application) V Secretary of State for the Department of Interior,[145] it was maintained that any retention beyond the stipulated need must be examined against potential damage to the privacy of the data subject. The ruling illustrated a judicial commitment to ensure that the retention practices are not excessive, imposing stricter limits regarding the expectations imposed on data controllers.

The divergence in the interpretations of the reasonableness between the 2019 DPA and the German law reveals a complex tapestry of regulatory approaches. The DPA establishes a relatively flexible framework that allows data controllers a certain latitude to determine retention periods while it is still anchored to the principle of need and proportionality. In contrast, the strict adhesion of the German law to the defined operational limits exposes a less flexible approach, which reflects a caution and calculated interpretation of reasonability.

This comparative analysis highlights the existing judicial and legislative nuances that shape the way in which reasonability between jurisdictions is operationalized, offering vital ideas about global dialogue about the retention and protection of data., The concept of duration of the retention of data is complex connected to the principles of necessity and reasonableness, acting as a rock substrate for the regulation of personal data by data and data processors. Pursuant to the data protection law, 2019, the duration for which personal data can be maintained must align with the purposes for which it has been collected, ensuring that they are not kept longer than necessary.

---

[144] Article 35, *Federal Data Protection Law* (BDSG)

[145] *R v Secretary of State for the Department of Interior, C-553/07,* The European Court of Justice (ECJ)

This closely reflects the German data protection framework, in particular as indicated in the Bundesdatenschutzgesetz (BDSG) and in the general regulation on data protection (GDPR), which emphasize similar doctrines of necessity and proportionality.

In the interpretation of what constitutes a "reasonable" duration for the consumption of personal data, both statutory and contextual factors must be considered. In the United Kingdom, the logic underlying data storage is often informed by the specific functions or purposes of the collection. For example, the data protection law, 2019 clarifies that personal data must be maintained only for all the time necessary to satisfy the purpose of the collection, after which they should be eliminated or anonymous. This principle promotes a dynamic understanding of "reasonableness", so the periods of retention of data can float on the basis of the variations of the specific operational needs of an organization.[146]

On the contrary, the German law, while adhering to the same fundamental principles outlined in the GDPR, incorporates a more prescriptive approach to data storage. According to BDSG, the conservation period must be outlined by relevant statutory regulations or justified by a convincing legitimate interest.[147] This manifests itself in a more rigorous evaluation of what constitutes a "reasonable" conservation period, often accompanied by times expressly defined by specific data categories. For example, the retention of financial data pursuant to German law can request the conservation of the documentation for a minimum of ten years, underlining a legal approach that requires compliance on contextual flexibility.[148]

In Germany, the Federal Constitutional Court has constantly declared that the storage of the data must be subjected to a rigorous test of necessity, in which storage beyond an established period must satisfy a high justification threshold.[149] For example, the maintenance of communication data required solid legal bases to justify the incursion in individual privacy.

---

[146] Veale M, Binns R, and Ausloos J, 'When data protection by design and data subject rights clash' *International Data Privacy Law*, 2018, 1-19 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081069 2018.
[147] Rustad ML and Koenig TH, 'Towards a global data privacy standard' *Florida Law Review*, 2019, 366- 453 https://www.floridalawreview.com/towards-a-global-data-privacy-standard 2019.
[148] Rustad, 'Towards a global data privacy standard,' 2019, 416.
[149] Sartor G and Lagioia F, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' European Parliament, Panel for the Future of Science and Technology (STOA), Study No. PE 641.530, 2020, 1–80 – https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN, April 2020.

Ultimately, the nuanced understanding of "reasonable" duration for the retention of data pursuant to the data protection law, 2019 and German law highlights a significant disparity in the operation of the principles of data protection. While both share a commitment to minimize data, the methodologies used to ascertain and apply reasonable retention periods reveal various degrees of statutory regulation and judicial supervision. The implications of these differences deserve careful consideration, in particular in an increasingly globalized panorama of data in which transfrontier data transfers require the harmonization of conservation practices and compliance obligations.[150] The advent of emerging technologies, particularly artificial intelligence (AI) and Big Data analysis, significantly influenced data retention practices between controllers and data processors. The 2019 data protection law, together with the German data protection law, had to adapt to these rapid technological advances, particularly in defining the concepts of "reasonable" and "necessary" in the context of data retention.[151] This assessment will elucidate how legal structures are responding to the challenges presented by AI and consequent implications for data retention.

The Data Protection Law, 2019, articulates specific requirements regarding personal data retention, highlighting the need for retention for specified and legitimate purposes. However, as AI technologies are increasingly dependent on vast amounts of data to develop and refine algorithms, the interpretation of "necessary" undergoes a paradigm shift.[152] AI development usually requires extensive data sets that can overcome what is traditionally considered reasonable under previous data retention standards. In this context, the law requires that the data should not be retained longer than necessary for the purpose for which it was collected, causing a reassessment of what is a legitimate goal at a time when the increased data through IA Plays a critical role in various sectors.[153]

In German law, the Federal Data Protection Law (BDSG) and the General Data Protection Regulation (GDPR) echo similar feelings, particularly in relation to the principles of data minimization and limitation of purpose. The cases of German jurisprudence illustrated the tension between broad data requirements for AI training models and legal data retention expectations. Notably, the Federal Court emphasized in several decisions the need for a clear justification for

[150] Sartor G, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 33.
[151] Sartor G, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 33.
[152] Sartor G, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 39.
[153] Sartor G, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 41.

retention periods, stating that any data retention strategy should explain the specificities of data processing activities.[154] This aligns with the German ethos of strict data protection, which requires that data controllers exercise caution and rigor to justify their retention practices in the context of AI use.

As AI technologies usually take advantage of historical data for predictive analysis, the issue arises if the retention of such data aligns itself with the principle of need incorporated into the 2019 Law and German Law. The legal scenario was previously oriented for concrete and defined purposes for data collection, but the complexities introduced by AI require a more subtle interpretation.[155] Dependence on historical data patterns implies potential data retention that can be considered excessive or disproportionate under traditional interpretations of reasonableness.

In light of these considerations, regulators on both sides of the spectrum are exploring structures that address the interaction between AI and data retention. For example, the introduction of data retention impact assessments in the 2019 Law seeks to ensure that data controllers and processors systematically evaluate their recently adopted technology data practices.[156] (Sartor & Lagioia, 2020). Similarly, Germany's regulatory bodies are advocating guidelines that encourage companies to adopt data protection by design, ensuring that AI solutions incorporate compliance with data retention patterns from the start to the full life cycle of the data.

Overall, the integration of AI into data retention practices requires a recalibration of legal definitions and guidelines to ensure that the principles of data protection maintain integrity in the midst of technological progress. Both the data protection law, 2019 and German law face fundamental challenges to balance the demands of innovation with the inviolability of individual data rights. As such, continuous dialogue between legislators, technologists and privacy advocates will be critical as these legal structures evolve to meet contemporary realities. The analysis of reasonable and necessary data retention within the structure of German law reveals a differentiated evolution shaped by significant judicial decisions that emphasize proportionality and necessity. Central to understand the application of these concepts under the data protection law, 2019, is the

[154] Brkan M, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' International Journal of Law and Information Technology, 2019, 91-121 – https://doi.org/10.1093/ijlit/eaz006 2019.
[155] Brkan M, 'Do algorithms rule the world' 2.
[156] Sartor G, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' 73.

jurisprudence established by the Federal Constitutional Court of Germany (BundesverFuSungsGericht - BVERFG), whose decisions had deep implications for data retention practices by controllers and processors of data.

In a constitutional complaint against section 113a and 113b of the Telecommunications Act (Telekommunikationsgesetz - TKG) as amended by the Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation.[157] The Court considered that the indiscriminate and general surveillance of communications, particularly in relation to the retention of personal data, violated the fundamental rights of individuals guaranteed by the Basic Law (GRUDSETZ). This decision emphasized the need for a rigorous legislative structure that dictates that data retention should be limited to what is reasonable and "necessary" to the purpose of law enforcement and public security. The decision emphasized an act of balance between state interests and individual privacy rights, establishing a clear precedent that favors the retention of limited data.

Subsequently, BVERFG's decision in the case related to the Data Retention Law (TelekomMunikatiSüberwachungs -Und -Speichegetz, or TKG) reaffirmed this principle by overturning provisions that allowed extensive data retention without adequate justification. This decision clarified that any retention should adhere to the criteria of necessity and proportionality, which means that data should only be retained when specific conditions are met, such as the existence of a concrete threat or specific research needs.[158] Such substantial decisions obliged legislative bodies to review existing data protection laws and communicate these standards in accordance with the EU letter of fundamental rights.[159]

In addition, a substantial influence on the decisions of the Court of Justice (TJA) of Europe arose, particularly in the case of Digital Rights Ireland Ltd. v. Minister of Communication, who echoed the logic of the German courts on too many data retention laws. After this European context,

---

[157] *Bundesverfassungsgericht, 1 BvR 256/08*, 2010

[158] Hoffmann W, Latza U, Baumeister SE, Brünger M, Buttmann-Schweiger N, Hardt J, and Hoffmann V, 'Guidelines and recommendations for ensuring Good Epidemiological Practice (GEP)' *European Journal of Epidemiology*, 2019, 302- 314, https://www.researchgate.net/publication/331500563_Guidelines_and_recommendations_for_ensuring_Good_Epidemiological_Practice_GEP_a_guideline_developed_by_the_German_Society_for_Epidemiology 2019.

[159] Hoffmann W, 'Guidelines and recommendations for ensuring Good Epidemiological Practice' 307.

German courts interpreted these decisions to impose more strict controls on personal data retention and processing. The implications of these interpretations extend to policy developments that prioritize privacy and safeguarding personal data consistent with the principles incorporated in GDPR.

In addition, jurisprudence began an informed dialogue between policy formulators, scholars and professionals about the thresholds of necessity and reasonableness in surveillance practices.[160] This dialogue leads to the reevaluation of administrative practices, reflecting a change towards a culture of responsibility and transparency between controllers and data processors. In the space of data retention policies, this reflection has materialized in efforts to prototypically and implement design privacy structures, which actively consider the principles of data minimization since the beginning of policy formation.[161]

The judicial scrutiny of data retention practices in Germany illustrates a broader commitment to defend individual rights against the invasion of the state, while at the same time meets the legitimate needs of law enforcement. It manifests itself in a rigorous application of the concepts of reasonable and necessary, serving as a legacy of German legal philosophy and a necessary component in the continuous evolution of the data protection law in the European context. Thus, German jurisprudence contributes not only to the interpretation of specific provisions in accordance with the Data Protection Law, 2019, but also enriches the discourse around data retention practices across Europe, defending robust data protection personal aligned with constitutional principles., The evolutionary overview of data protection has required the establishment of solid frameworks aimed at guaranteeing compliance with regulations, particularly in relation to the principles of retention of reasonable and necessary data. Data protection officers (DPO) play a fundamental role in the guidance of organizations towards compliance with these principles under the Data Protection Law, 2019 (DPA 2019) and, according to the German law based on in the General Regulation of Data Protection (GDPR). The multifaceted responsibilities of the DPO extend beyond mere compliance controls; They have the task of promoting a culture

[160] Hintze M, 'Viewing the GDPR through a de-identification lens: A tool for compliance, clarification, and consistency' *International Data Privacy Law,* 2018, 1-22 – https://ssrn.com/abstract=2909121, 2018.
[161] Hintze M, 'Viewing the GDPR through a de-identification lens' 17

of data protection within their organizations, which is inherently linked to the internal protocols that govern data governance.

According to the 2019 DPA, the appointment of a DPO is mandatory for certain data processors and data processors, which reflects a similar obligation established within the GDPR.[162] The DPO is essential to ensure that data retention practices are aligned with the principles of need and proportionality, which are at the heart of both legal frameworks. A practical example of this implies the implementation of the retention schedules that specify the duration for which several data categories can be retained. These schedules must be rooted in a deep understanding of the aims for which the data is collected and processed. Therefore, effective organizational protocols must cover regular audits, evaluations and training to facilitate compliance and promote an understanding of the implications of data retention policies.

In German organizations, the integration of DPO in data governance structures has exhibited particular strengths, particularly in their systematic approaches for data minimization and retention policies. The German Federal Data Protection Law (BDSG) complements GDPR stipulations by providing more clarifications on the management of personal data.[163] Within this framework, DPOs are often integrated into corporate compliance equipment, allowing an interdisciplinary approach to the data government. This integration encourages an integral vision of data strategies that explain both regulatory compliance and commercial objectives, which finally allows organizations to implement the necessary retention protocols that are justifiable and aligned with broader corporate governance strategies.

In the context of comparing the two legal frameworks, it becomes clear that organizational protocols in German companies prioritize the meticulous documentation of data processing activities, which is crucial to demonstrate compliance with the principles of necessity and proportionality. Organizations generally use detailed data flow analysis and retention impact

[162] Clifford D, Graef I, and Valckl P, 'Pre-formulated declarations of data subject consent citizen-consumer empowerment and the alignment of data, consumer and competition law protections' *German Law Journal*, 2019, 679-721 – https://www.cambridge.org/core/journals/german-law-journal/article/preformulated-declarations-of-data-subject-consent-citizenconsumer-empowerment-and-the-alignment-of-data-consumer-and-competition-law-protections/ 2019.

[163] Urban T, Tatang D, Degeling M, Holz T, and Pohlmann N, 'A study on subject data access in online advertising after the GDPR' ESORICS 2019 International Workshops, Luxembourg, September 26–27, 2019, 61-79.

evaluations that involve interested parties of legal, technical and operational teams. This holistic approach facilitates a clearer understanding of the management and retention needs of the data life cycle. In addition, in cases of data violations or regulatory consultations, the strength of the existing documentation can mitigate the possible sanctions and risks of litigation.

On the contrary, while organizations that operate under the DPA 2019 are also encouraged to adopt similar best practices in data governance, implementation and adhesion levels can vary widely. The emphasis placed on the functions of DPO and organizational protocols may be influenced by the availability of resources and organizational culture. In many cases, the role of the DPO remains limited, which limits the ability of organizations to completely participate in proactive compliance efforts. Consequently, dependence on AD-Hoc or poorly defined data retention policies can lead to challenges to meet the requirements of the 2019 DPA, which could cause an inconsistent application of the retention principles.

Ultimately, the different legal and organizational landscapes have unique challenges and opportunities for data controllers and processors in both jurisdictions. The efficacy of the DPO and the underlying protocols within the organizations determines the degree to which they can maintain the principles of reasonable and necessary data, ensuring compliance with regulatory expectations while promoting confidence between interested parties in a increasingly complex environment based on data., The concepts of "reasonable" and "necessary" in the context of data retention under the 2019 data protection law are essential to determine the obligations of controllers and data processors. These concepts not only delimit the limits of the processing of legal data, but also guarantee that personal data is not kept beyond its planned objective, thus improving the rights to individual confidentiality. Comparative analysis with German law, in particular in the light of the previous ones of relevant cases, offers critical information on how these principles are operationalized in different legal systems.

In German law, the strict application of the principles of data minimization testifies to the country's historic commitment to protect personal data. The Federal Data Protection ACT (BDSG) is closely aligned with the European Data Protection Regulation (GDPR), stressing the need to justify the periods of data retention in clear and practical terms. Thanks to case law, the German judicial power has strengthened the importance of demonstrating that the preserved data is not simply

practical but indeed necessary to achieve specific and legitimate purposes. This judicial examination obliges data controllers and processors to develop robust data retention policies which are transparent, responsible and subject to a periodic examination.

The alignment of reasonable and necessary concepts of reason with statutory frameworks such as the 2019 data protection law and German law is used to harmonize data protection standards through the courts. This alignment is essential not only for compliance purposes, but also to promote an environment of trust between individuals and organizations. Data controllers and processors must adopt a proactive approach to data governance - that which incorporates confidentiality by design principles and operationalizes these legal concepts in practical data retention strategies.

For decision -makers, the challenge consists in establishing a unified regulatory framework that adapts to nuanced interpretations of reasonable and necessary retention of data while respecting the cultural and legal traditions of different jurisdictions. The recommendations for carrying out this harmonization include collaboration efforts to develop clear guidelines that define what constitutes a "reasonable necessity" in variable data processing contexts. In addition, the adoption of best practices from case law in Germany can provide a precious reference point for other jurisdictions that strive to consider data protection.

In addition, the emphasis should be placed on the importance of continuing education and awareness of data controllers and processors concerning compliance with data protection laws. This training should not only cover legal requirements, but also include ethical considerations surrounding data retention, thus promoting a more complete understanding of the implications of data processing actions.

Consequently, the implications for the alignment of reasonable and necessary practices of data conservation with the Data Protection Act and German law extend beyond simple regulatory compliance. They resonate with wider societal values based on the protection of individual rights and the ethical management of personal data. As data landscapes are evolving, promoting a culture of responsibility and transparency in data preservation practices will be essential for data controllers and processors, while serving as a director for future political decisions targeting to harmonize data protection standards worldwide.

CHAPTER 4

ENHANCING DATA RETENTION POLICIES IN KENYA: GUIDELINES AND BEST PRACTICES

4.1 Introduction

In the digital age, the importance of robust data retention policies cannot be exaggerated, particularly in a rapidly developing country, such as Kenya, where the intersection of technology, privacy and governance increasingly shapes the lived realities of individuals and the Operation of organizations. Data retention policies determine the time that personal data is maintained and the way it is dealt with, significantly influencing individual's privacy rights, the security of sensitive information and the effectiveness of governance structures in the public and private sectors.[164]

As the volume of data generated and processed continues to expand exponentially due to technological advances, the need for effective personal data management becomes fundamental. In an environment characterized by frequent data violations and unauthorized data sharing, clear data retention protocols can mitigate potential risks.[165] Personal data, being inherently sensitive, presents challenges related to unauthorized disclosure and misuse of information. This emphasizes the importance of establishing comprehensive guidelines that not only govern the duration of retention, but also ensure that organizations are responsible for the data they collect and retain.[166]

4.2 Proposed Guidelines for Kenya

The implications of data retention policies extend beyond the individual to cover broader social considerations. With advances in data analysis and artificial intelligence, the potential for surveillance and the comprehensive control of citizens through extensive data collection practices

---

[164] Mukuki A and Assenga A, 'Comparative study of data protection legislation frameworks across the East African community' Strathmore University, March 2024, 1-38 – https://www.google.com/url?sa=i&url=https%3A%2F%2Fcipit.org%2Fwp-content%2Fuploads%2F2024%2F11%2FCross-Border-Data-Flows-in-Africa-Exploring-Legal-Frameworks-and-Regional-Importance-1_compressed.pdf&psig=AOvVaw0lOZGGF57sPUOm9fFxlTFc&ust=1746030812137000&source=images&cd=vfe&opi=89978449&ved=0CAQQn5wMahcKEwjI3N2R1_2MAxUAAAAAHQAAAAAQBA

[165] Mukuki A, 'Comparative study of data protection legislation frameworks across the East African community,' 33.

[166] Mukuki A, 'Comparative study of data protection legislation frameworks across the East African community,' 28.

has ethical and significant governance dilemmas. In Kenya, a country where the commitment to freedoms and personal privacy is enshrined in the Constitution, the absence of well -defined data retention policies can result in allowing practices that undermine public trust in institutions. This situation exemplifies the urgent need for improved structures that prioritize the rights of individuals while meeting the operational needs of organizations.

In this context, the principles of data protection and privacy must be harmonized with the realities of technological capacities and the imperatives of governance. Recommended data retention practices should therefore adopt a double focus to ensure that personal data is retained only for the time required for the intended purpose when implementing measures that ensure safe handling and deletion of data when no longer needed. These measures include:

Clear Categorization of Data Sets

1. *Data Classification*: This involves categorizing data based on its sensitivity and importance. For instance, sensitive data such as financial information or health records requires stricter safeguards than less sensitive data like contact details.[167] The African Union's Data Policy Framework emphasizes the importance of categorizing data to ensure appropriate protection levels, aligning with principles like those in the GDPR, which mandates that data processing be lawful, fair, and transparent.[168]
2. *Purpose Specification*: Each category of data should be linked to specific purposes for which it is collected and processed. This ensures that data is not used beyond its intended scope, aligning with the principle of purpose limitation in data protection regulations.[169]

Retention Schedules

1. *Time Limits for Data Retention*: Establishing clear retention schedules ensures that data is not kept indefinitely. This involves setting specific time limits based on the purpose of

[167] Yusuf B, 'Harmonization of Data Governance Frameworks in Africa' Centre for International Governance Innovation, Digital Policy Hub, 2024, 1-7 https://www.cigionline.org/documents/3133/DPH-paper-Yusuf_3HvhA8r.pdf April, 2024.
[168] *African Union: AU Data Policy Framework,* 2023.
[169] *United Nations; Principles on Personal Data Protection and Privacy*, High-Level Committee on Management (HLCM), 2018.

data collection and legal requirements. For example, the GDPR requires that personal data be kept for no longer than necessary for the purposes for which it was collected.[170]

2. *Regular Review:* Regular reviews of retention schedules are essential to ensure that data is not retained beyond its usefulness. This process helps in identifying data that can be safely deleted or archived, reducing storage costs and minimizing privacy risks.[171]

Data Disposal Procedures

1. *Secure Deletion Methods:* Data disposal procedures must ensure that personal data is securely deleted when no longer needed. This includes using methods like encryption, secure erasure, or physical destruction of storage media to prevent unauthorized access.[172]
2. *Documentation of Disposal:* Keeping records of data disposal is crucial for accountability and compliance with data protection regulations. This documentation helps in demonstrating adherence to legal standards and internal policies.[173]

Such structures should be based on international precedents, such as those found in German law, where strict data protection regulations usually serve as guiding models to balance individual rights and state interests.

In addition, the involvement of stakeholders is crucial in the development and operationalization of effective data retention policies. Involving the main stakeholders - such as government agencies, private sector entities, civil society organizations and the general public - are considered several perspectives, facilitating the creation of inclusive guidelines that reflect the unique social, cultural and economic contexts of Kenya. Through collaborative dialogues, stakeholders can share insights and best practices, promoting a culture of responsibility and transparency in data management.

Thus, the development of comprehensive data retention policies in Kenya requires a multifaceted approach that emphasizes personal data protection, sensitive information security and effective governance promotion. By integrating legal recommendations, advanced technological solutions and inclusive stakeholder engagement, Kenya can improve its data retention structures, aligning

---

[170] Yusuf, B, 'Harmonization of Data Governance Frameworks in Africa,' 7.
[171] *United Nations Guidance Notes; Data Privacy, Ethics and Protection*; High-Level Committee on Management (HLCM), 2018.
[172] Yusuf B, 'Harmonization of Data Governance Frameworks in Africa,' 7.
[173] *United Nations; Principles on Personal Data Protection and Privacy*, High-Level Committee on Management (HLCM), 2018.

them with global standards and practices, as well as defending the fundamental rights of their citizens., In Kenya, the legal framework that governs data storage is anchored mainly in the Data Protection Act, 2019, which provides a detailed directive on the processing of personal data within the jurisdiction. This law was basically influenced by the Constitution of Kenya, 2010, which guarantees the right to privacy. The law establishes several key principles aimed at safeguarding the personal information of people, the provisions for the rights of data subjects and the responsibilities of controllers and data processors.[174] In addition, the Office of the Commissioner for Data Protection (ODPC) was set up to supervise the application of these regulations, ensuring that the organizations comply with the measures established by the data protection.[175]

4.3 Challenges and Gaps within the Current framework

Several gaps and challenges within the current data storage framework remain evident. Firstly, while the data protection law provides a solid basis, it lacks specific guidelines relating to data storage periods, leading to inconsistent practices in various sectors.[176] The absence of clearly defined times for the conservation of personal data can contribute to both the excessive retention and the sub-surrender of the data, creating potential risks in the compliance and management of ethical data.[177] These ambiguity can also lead to non -intentional violations of privacy rights, raising concerns between the parties concerned regarding responsibility.[178]

Secondly, the interaction between the data protection law and the various specific regulations of the sector that regulate data storage continue to be problematic.[179] For example, several sectors, such as health, finance and telecommunications, have their own data management policies that could be in conflict with the principles established in the data protection law. This regulatory

[174] *Data Protection Act,* 2019.
[175] Mutua SN, and Zhang Y, 'Online content regulation policy in Kenya; Potential challenges and possible solutions' Journal of Cyber Policy, 2021, 177-195 – https://doi.org.ezproxy.library.strathmore.edu/10.1080/23738871.2021.1916974, published 2021.
[176] Mutua S, 'Online content regulation policy in Kenya,' 181
[177] Mutua S, 'Online content regulation policy in Kenya,' 181
[178] Mutua S, 'Online content regulation policy in Kenya,' 181
[179] Mutua S, 'Online content regulation policy in Kenya,' 182

fragmentation complicates compliance for organizations operating in several sectors, often causing a lack of clarity regarding legal obligations and data management responsibilities.[180]

In addition, the Opentive capacity of the ODPC remains a challenge. Although it has the task of the fundamental role of enforcing data protection laws, the office must face significant restrictions of resources that limit its ability to adequately monitor compliance and respond to data violations.[181] There is also a well -known deficiency in the awareness of the public regarding the rights and data protection obligations. The effective involvement of the interested parties is crucial to promote an environment in which organizations can navigate in the legal scene with confidence and citizens are informed about their rights, but this commitment is currently considerably inadequate.[182]

In addition, the proliferation of technology presents unique challenges that the current legal framework has not completely faced. The rapid progress of data processing technologies, such as artificial intelligence and Big Data analysis, requires adaptive legal measures that existing laws may not be sufficiently satisfied.[183] This disjunction between technology and regulation raises concerns about the effectiveness of data protection practices in safeguarding personal information in an increasingly digital society.[184]

4.4 Proposed Recommendations

Comparably, the lessons of the German law regarding the storage of data can offer valuable ideas in identifying the best practices and overcoming existing gaps. The German Federal Data Protection Act, which implements the European Data Protection Regulation (GDPR), provides clear storage standards and requires a significant commitment with the parties concerned through the assessments of data protection impact. Incorporate similar paintings within the Kenya legal scene could improve compliance and strengthen data protection mechanisms.

---

[180] Mutua S, 'Online content regulation policy in Kenya,' 182
[181] Mutua S, 'Online content regulation policy in Kenya,' 182
[182] Mutua S, 'Online content regulation policy in Kenya,' 182
[183] Mutua S, 'Online content regulation policy in Kenya,' 182.
[184] Mutua S, 'Online content regulation policy in Kenya,' 182.

In summary, while Kenya made great strides in establishing a legal framework for data storage through the data protection law, the challenges relating to the inconsistencies in the regulations, in the operational capacity, the awareness of the public and in technological progress persist . Tackling these gaps is essential for the development of a complete and effective data storage policy that not only aligns international standards, but also promotes the trust between the parties concerned in the management of personal information. The data conservation policies emerged as a fundamental focus for jurisdictions all over the world while dealing with the double imperative to safeguard personal data and guaranteeing its availability for law enforcement and national security purposes. In examining the best practices for data storage policies in Kenya, it is prudent to examine the approaches adopted both by his neighbors of Eastern Africa and by more established legal paintings in Europe, in particular Germany. The comparative analysis reveals crucial insights that can serve to strengthen Kenya data strategies.

A remarkable practice is the principle of data minimization, which requires organizations only to retain the necessary data for specific and legitimate purposes. This principle was fundamental to reduce unnecessary data storage and mitigate risks associated with data violations.[185] For Kenya, the adoption of similar guidelines can promote a cultural change for responsible data management, ensuring that data retention policies are aligned with specific organizational mandates and regulatory requirements.[186] This alignment is particularly crucial in a country where misuse of data can exacerbate the existing challenges related to privacy and security.

In Germany, rigorous transparency requirements require organizations to inform users about their data retention policies at the data collection point. Users also have the right to understand how their data will be used and retained, along with the corresponding deadlines.[187] The implementation of such transparency measures in Kenya can significantly improve public trust in data collection

[185] Schade J, 'Kenya "Olkaria IV" Case Study Report; Human Rights Analysis of the Resettlement Process' Centre on Migration, Citizenship and Development (COMCAD), Working Paper Number 51, 2017, 1-171 https://www.ssoar.info/ssoar/bitstream/handle/document/51409/ssoar-2017-schade-Kenya_Olkaria_IV_Case_Study.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2017-schade-Kenya_Olkaria_IV_Case_Study.pdf 2017.

[186] Schade J, 'Kenya "Olkaria IV" Case Study Report; Human Rights Analysis of the Resettlement Process' 60.

[187] Inau ET, Nalugala R, Nandwa WM, Obwanda F, Wachira A, and Cartaxo A, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya' *Data Intelligence*, 2022, 853 – 862 https://direct.mit.edu/dint/article/4/1/162/109905/Fair-Equivalency-Regulatory-Framework, 2022.

processes and generate a more informed user base. Establishment of clear communication channels and user rights on data retention would reinforce the responsibility between processors and data controllers.

In addition, the German system is based on regular audits and evaluations to ensure compliance with data retention policies. Audit practices in Germany involve internal and external evaluations, which help identify non -compliance problems and areas of improvement.[188] Kenya can benefit from the institution of similar audit structures that allow consistent monitoring and application of data retention practices, thus ensuring adherence to the established guidelines. The involvement of independent auditors can strengthen the integrity of these evaluations, thus increasing the confidence of stakeholders in the effectiveness of data management structures.

Technology also plays a key role in the German approach to data retention. Digital solutions, such as automated data life cycle management systems, are used to facilitate secure and efficient data storage.[189] These systems automate data deletion after the specified retention period, thus maintaining the data minimization principle and reducing human error.[190] The adoption of such technological solutions in Kenya would not only optimize compliance with retention policies, but would also mitigate the administrative load on the organizations required to focus on data protection.

The involvement of stakeholders is essential in the Kenyan structure, where a collaborative approach involving government agencies, private sector organizations and civil society groups were established.[191] These stakeholders work together to develop, implement and refine data protection standards.[192] Similarly, in Kenya, the cultivation of a forum of several stakeholders can facilitate dialogue and knowledge sharing between various parties involved in data processing and

[188] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 854.
[189] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 855.
[190] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 856.
[191] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 858.
[192] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 859.

retention. The establishment of such platforms could encourage various perspectives in the development of policies that address the unique socioeconomic context of Kenya.

Precedents of German law also demonstrate the effectiveness of comprehensive data retention regulations. The Federal German Data Protection Law (BDSG) complements GDPR, providing additional protection layers and a clearer structure for retention policies that meet specific sectors.[193] Drawing BDSG parallels, Kenya can be encouraged to develop specific sector guidelines that meet the different data management needs in different industries, ranging from medical assistance to telecommunications. This personalized approach would allow more effective regulatory supervising mechanisms and encourage the compliance of various sectors in the Kenyan economy.

Through the synthesis of these best practices of the German legal structure, Kenya has the opportunity to reformulate their data retention policies. Focusing on data minimization, transparency, audit practices, technological solutions, involvement of stakeholders and industry - specific guidelines offers a multidimensional strategy for creating a robust data retention structure that aligns with international standards. The implementation of these recommendations can place Kenya on a way to improve governance and data protection, ultimately protecting the rights of their citizens and promoting a safer digital environment., The integration of technological solutions into data retention policies in Kenya has the potential to significantly improve the management, safety and compliance of data management practices in various sectors. The center of this effort is cloud storage, data encryption and safe management of the data life cycle, all of which are fundamental to address the multifaceted challenges raised by data retention regulations while guaranteeing the Compliance with existing legal frameworks.

Cloud storage

Cloud storage represents a transformative change in the way organizations manage and store data. The flexibility and scalability of cloud solutions allow organizations to efficiently administer large amounts of data while adhere to retention requirements.[194] When adopting cloud services,

[193] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 859.

[194] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 860.

organizations can minimize overloads associated with physical storage infrastructure, thus redirecting resources towards central operations.[195] In particular, cloud suppliers often offer improved compliance characteristics that are aligned with local and international data protection regulations, which facilitates Kenya organizations to develop and implement data retention policies that meet the legal standards. In addition, leading cloud service providers use advanced data redundancy mechanisms to ensure that information is not only safely stored but also recoverable in case of data loss, which supports the continuity of the organization.[196]

Data encryption

Data encryption is another critical technological solution that can reinforce data retention practices. As data violations become more and more frequent, the importance of protecting confidential information cannot be exaggerated. By encrypting both rest and transit data, organizations can mitigate the risk of unauthorized access and ensure that consistent retention practices do not compromise data security.[197] The encryption serves as a robust barrier against possible adversaries, thus promoting an environment of trust between interested parties, including consumers and regulatory bodies. In addition, regulatory frameworks, such as the General Data Protection Regulation (GDPR) in Europe, recognize encryption implementation as a mitigating factor in the instances of data infractions, which could influence similar provisions in the legislation of protection of data.

System Development Life-Cycle Management (SDLM)

The safe management of the data life cycle (SDLM) covers the integral management of the data of its creation and storage to its eventual elimination.[198] The implementation of SDLM practices allows organizations to establish clear protocols for the retention of data that are aligned with legal

[195] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 860.
[196] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 860.
[197] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 861.
[198] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 861

obligations while improving operational efficiency.[199] An effective SDLM frame incorporates automated classification and data labeling, ensuring that the information is classified according to its retention requirements.[200] This not only simplifies compliance, but also facilitates responsible elimination of data that are no longer required, thus reducing the risks associated with the unintentional exposure of confidential information.[201] The development of SDLM systems can also be informed by the precedents of the German law, which integrates strict data protection standards in their frameworks, which guarantees that individual privacy rights are constantly maintained throughout the entire life data cycle .

In addition, the integration of these technological solutions requires the participation of interested parties, since organizations must collaborate with technology suppliers, legal consultants and regulatory agencies to guarantee a holistic approach to data retention policies. Interesting interested parties ensure that technological implementations adapt to specific jurisdictional requirements while promoting an environment of responsibility and transparency in data management practices.

In summary, the adoption of cloud storage, data encryption and safe management of the data life cycle represents not only a progressive approach to improve data retention practices in Kenya, but also an imperative response to the panorama in Evolution of digital information security.[202] The establishment of these practices, informed by international standards and local legal precedents, is crucial to develop a solid framework that aligns organizational operations with legal demands while building public confidence in data management practices.[203] These advances will play a fundamental role in the configuration of a resistant and responsible data governance framework in Kenya., The development of solid data retention policies requires an active and significant

[199] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 862.
[200] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 860.
[201] Inau E, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya,' 860.
[202] Koeva M, Stöcker C, Crommelinck S, Ho S, Chipofya M, Sahib J, and Bennett R, 'Innovative remote sensing methodologies for Kenyan land tenure mapping' *Remote Sensing,* 2020, 1-27 https://www.mdpi.com/2072-4292/12/2/273,17 January 2020.
[203] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, October 2023,1–46.

commitment of several stakeholders, including government entities, private companies and civil society. The commitment of stakeholders provides a framework to create inclusive policies that are fair, effective and reflect various perspectives and needs.[204] Multisectoral commitment not only requests various points of view but also improves the legitimacy and conformity of the emerging policies.[205]

Government Stakeholders, Private Companies and Civil society organizations (CSO) Cooperation

Government organizations play a central role in the formulation of data retention policies, as they are responsible for ensuring that laws and regulations respect national and international legal frameworks.[206] The involvement of government stakeholders can promote transparency and responsibility. For example, decision -makers can benefit from the information collected from legal practitioners concerning the applicability of existing laws and the implications of the regulations proposed on confidentiality and data protection rights. This collaborative approach can also prevent the potential legal challenges or legal challenges that may arise during implementation. In addition, the government's commitment promotes public confidence by ensuring that policies are developed in the public interest, reflecting societal values and expectations.

Private companies are also crucial in dialogue surrounding data retention policies. As main guards of large amounts of data, companies have unique information on technical, operational and logistical challenges linked to data retention.[207] Committing to the stakeholders in the private sector allows political decision -makers to discuss the best practices that these entities have adopted, ensuring that policies take into account the realities of data management and collection practices in the environment of business. In addition, private companies often bring technological solutions to the table, including the progress of data storage and encryption that can improve compliance with retention policies while protecting the confidentiality of individuals.

[204] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 15.
[205] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 30.
[206] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 25.

[207] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 32.

Civil society organizations (CSO) represent another vital district in the development of data retention policies. These groups often serve as defenders of individual rights and freedoms, ensuring that policies promote not only the interests of the State and the affairs, but also the fundamental rights of citizens.[208] Civil society actors can provide a critical analysis of how data conservation policies can disproportionately affect vulnerable populations. Their involvement can help highlight potential ethical problems and guarantee that policies are sensitive to human rights considerations.[209] In addition, CSOs can facilitate community engagement, serving as a bridge between decision -makers and the general public to promote understanding and collect basic comments on data retention problems.

An inclusive approach to stakeholders' commitment recognizes that no sector has all the responses to the complexities of data retention.[210] The previous ones established in jurisdictions like Germany, which emphasizes a balance between data usefulness and privacy rights, illustrate the advantages of collaborative governance. Germany has sought to initiate stakeholders from various sectors - government, industry, academic and civil society - in discussions concerning the protection and retention of data. This commitment has shaped robust frameworks that are adaptable over time and reactive to technological changes.

In the end, the progress of data retention policies in Kenya can be considerably improved thanks to the full commitment of stakeholders. This approach facilitates the gathering of a complete range of ideas and expertise, helping to create complete, fair and enforceable policies. Consequently, it is imperative that Kenya adopts mechanisms to institutionalize the engagement of stakeholders in the process of elaboration of policies, drawing lessons from successful international previous ones while adapting these practices to the local context.

[208] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 37.
[209] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 38.
[210] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 42.

Legal Structure Reform

In the context of the improvement of data retention policies in Kenya, it is imperative to explore a multifaceted approach that intertwines legal reform and regulatory supervision. Legislative efforts must be made to establish a robust structure that articulates clear data retention obligations, respecting individual privacy rights, adhering to international standards and meeting local needs.

Currently, the Kenyan data protection scenario describes the principles for the processing of personal data. However, to strengthen the legal foundations of data retention policies, it is crucial to change existing legislation to ensure specificity in relation to retention periods for different data categories.[211] Establishing these parameters can help mitigate the ambiguity that currently involves retention practices, thus increasing compliance between controllers and data processors.

A recommended legislative reform is the introduction of a statutory structure that differentiates data retention requirements based on the data type that is being processed personal, sensitive or non-personal. This may be based on the example of the Federal Data Protection Law of Germany, which prescribes retention periods that align with the intended purposes of data processing. This targeted approach would promote a clear understanding among organizations about their responsibilities, facilitating better compliance and responsibility.

In addition to reforming the legal structure, the improvement of regulatory supervision is critical. The Office of the Data Protection Commissioner (ODPC) in Kenya has the task of ensuring compliance with the data protection law; However, its capacity must be reinforced to effectively monitor data retention practices in various sectors. Improved supervision mechanisms may include regular audits, compliance checks and establishing a reporting obligation for data violations related to adhering to retention policies. Involving stakeholders' consultations and ensuring that ODPC has proper financing and resources to perform its regulatory functions will significantly contribute to a more effective supervision environment.

[211] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 44.

In addition, promoting collaboration between agencies can facilitate a synergistic approach to regulatory supervision. The main stakeholders, including the ODPC, the Kenya Communication Authority and other relevant government and non-governmental bodies, must be involved in an exchange of best practices and intelligence. This may be inspired by the German data protection model, where collaboration between regulatory authorities at various levels increases the effectiveness of data governance.

The promulgation of penalties for non -compliance is not only as an impediment, but also enhances the general structure of responsibility. A layer penalty system, similar to what can be observed in the European Union's General Data Protection Regulation (GDPR), would provide clarity on the branches of not following the retention guidelines. In this sense, it is advisable that Kenya considers instituting increasing fines that reflect the severity and nature of the violation, along with the size and resources of the organization.

To support these legal recommendations, the cultivation of a culture of conformity through educational initiatives and awareness campaigns is crucial. Intempted engagement programs that promote understanding of data retention responsibilities can further solidify the commitment to ethical data management practices. The establishment of advisory committees involving representatives from various sectors - including academia, civil society and industry - would reinforce the essential collaborative effort to provide tangible improvements in data retention policies.

In short, legislative reforms complemented by enhanced regulatory supervision and stakeholder involvement provide a comprehensive approach to strengthen data retention policies in Kenya. By integrating best practices with local and international legal structures, particularly those established by German law, Kenya can cultivate an ecosystem conducive to responsible data management while protecting individual privacy rights.

Collaboration

The associations between the government and the private sector play a fundamental role in promoting innovation and responsibility in data retention strategies within Kenya. The complex and evolutionary panorama of privacy and data retention requires collaborative frameworks that

can efficiently take advantage of technological advances while guaranteeing compliance with legal guidelines. Public-private partnerships (PPP) underlined can significantly improve data management and retention capacity, ultimately improving the general integrity of data management processes.[212]

To begin with, the government must interact with technology companies to develop solid data storage solutions that adhere to local and international standards for data retention.[213] These associations can facilitate the implementation of avant -garde technologies, such as cloud storage and block chain, which offer better safety, scalability and data accessibility. For example, Blockchain adoption could provide immutable records for data management, improving responsibility between stakeholders in several sectors. In addition, the integration of artificial intelligence can optimize data classification and retention methodologies, thus simplifying compliance with regulatory requirements while improving operational efficiency simultaneously.

In addition, the participation of interested parties is essential in the establishment of effective data retention policies. Involving private sector entities, especially those with experience in data analysis and cybersecurity, can lead to the formulation of guidelines that are practical and innovative.[214] Through collaborative dialogues, several interested parties, including government agencies, civil society organizations and private companies, can address concerns related to data privacy, regulatory compliance and operational challenges. This inclusion will strengthen the legitimacy and acceptance of policies among all parties involved, promoting a culture of responsibility.[215]

The legal recommendations that revolve in successful models such as those of German law provide a framework within which Kenya's policies could develop. The rigorous approach of Germany for data protection, established through the General Data Protection Regulation (GDPR), highlights the importance of comprehensive legal frameworks to guide data retention practices. By building associations that focus on legal literacy, Kenya's interested parties can work in collaboration to

[212] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 15.
[213] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 23.
[214] Mutua S, 'Online content regulation policy in Kenya,' 189.
[215] Mutua S, 'Online content regulation policy in Kenya,' 189

adapt the German principles relevant to local contexts. These adaptations may include the establishment of clear parameters for the duration of data retention, the rights to people with respect to their data and strict sanctions due to breach, elements that can improve the execution and effectiveness of the data retention strategies of data from Kenya.

In addition, it is essential to promote a culture of responsibility within government and private sectors. Responsibility mechanisms can be reinforced through regular audits and evaluations of data retention practices, as well as transparency in the results of reports to both the authorities and the public. Public-Private associations must prioritize the formation of transient organisms, which include representatives of the government, industry and civil society, responsible for monitoring and evaluating adherence to data retention policies, thus ensuring that both sectors are responsible for their roles in the data life cycle.[216]

In addition, the development of continuous capacities through training and workshops is essential to ensure that all interested parties are up to date with the best practices in data management and management. Educational initiatives must focus on the implications of data protection laws, available technological tools and ethical considerations on data use and retention. By equipping interested parties with the necessary skills and knowledge, Kenya can develop a highly competent workforce capable of effectively navigating complex data retention landscapes.

In essence, the promotion of associations between the Government and the private sector in Kenya presents a strategic opportunity to advance data retention practices. By integrating innovations, improving legal frameworks, promoting responsibility and guaranteeing a solid participation of interested parties, Kenya can develop data retention policies that are comprehensive and adaptable to the digital environment that changes rapidly.[217] In recent years, data retention structures in various Kenyan institutions have obtained significant scrutiny, particularly in relation to their ability to ensure efficient registration maintenance practices and data management. A review of existing structures reveals various inconsistencies and inadequacies that prevent ideal data management. Many institutions do not adhere to systematic data retention policies, leading to

[216] Mutua S, 'Online content regulation policy in Kenya,' 190
[217] Mutua S, 'Online content regulation policy in Kenya,' 189.

disorganized and fragmented repositories that complicate access, usability and compliance with possible legislative requirements.[218]

4.5 Conclusion

Finally, looking at the precedents established within the German law, in which rigorous data protection standards and storage are incorporated into a complete legal framework, Kenya could align its policies with international standards by addressing local needs. German approaches exemplify a commitment to balance data innovation with rigid guarantees of privacy, underlining a path that Kenya could consider perfecting its data storage policies.

Ultimately, the intersection of the best environmental management practices and the governance of data has a promising path to improve data storage policies in Kenya. By adopting strategies focused on the commitment of the interested parties, clarity in roles, technological integration, continuous improvement, transparency and best international practices, Kenya can establish a robust picture for the management of its data responsible and effectively. The evolution of the digital landscape in Kenya highlights the urgent need for improved data retention policies, integrating a multifaceted approach that includes legal frameworks, technological innovations and the commitment of stakeholders. In particular, a consolidated strategy must reflect the complexities of data management in contemporary society while guaranteeing compliance with global standards.

Legal recommendations are essential in this context, in particular in the light of international best practices derived from jurisdictions such as Germany, where strict data protection laws strengthen the importance of legal data retention. The Federal Data Protection Act of Germany provides a robust framework that emphasizes the need for explicit consent and guarantees that the data is only kept For a long time that is necessary for its planned ends. For Kenya, the adoption of similar legislative measures would facilitate responsibility and transparency, ensuring that public and private entities respect the complete data retention protocols.

Technological solutions must also play a crucial role in improving data retention policies. The implementation of secure storage systems, data encryption techniques and automated data life

[218] Mutua S, 'Online content regulation policy in Kenya,' 190.

cycle management can considerably optimize data governance. In addition, the adoption of cloud -based services with strict compliance features will support data integrity and accessibility, aligning with international best practices. In addition, taking advantage of artificial intelligence (AI) for data analysis can provide information on retention needs, helping organizations to determine essential data and which can be rejected according to regulatory requirements.

Stakeholders' commitment is also critical in these companies. The Kenyan government must promote collaborations between various stakeholders, including telecommunications companies, financial institutions, civil society organizations and the general public. These partnerships can facilitate a better understanding of local data retention needs, cultural contexts and ethical considerations.[219] Participatory executives who integrate the comments of the stakeholders will ensure that policies are relevant and will effectively take up unique challenges faced by citizens and businesses.[220] The commitment of various stakeholders in the policy formulation process improves not only the legitimacy of the data retention framework, but also promotes collective responsibility for data stewardship.

Considering these elements, it becomes more and more clear that the approach of Kenya on data retention policies must adopt a more integrated perspective. Future research should explore how other jurisdictions have discussed similar challenges and consider cultural, economic and social nuances specific to Kenya. Such explorations will help refine policy proposals and adapt successful strategies from international previous ones.

To summarize this analysis, Kenya is held at the crossroads of an important opportunity to strengthen its data retention policies. Thanks to a mixture of complete legal approaches, advanced technological solutions and inclusive engagement of stakeholders, it is possible to create a resilient framework which embodies the principles of responsibility, security and respect for individual confidentiality. This requires not only political innovation but a sustained commitment from all sectors of the company to ensure that data preservation practices are effective, fair and aligned on the aspirations of a digital future. As the discussion progresses, it is imperative that attention for

[219] Mutua S, 'Online content regulation policy in Kenya,' 189.
[220] Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, 42.

future research remains focused on these critical intersection points, promoting a collaborative environment for improvement.

CHAPTER 5

FINDINGS, RECOMMENDATIONS AND CONCLUSIONS

5.1 Introduction

This chapter highlights the study's conclusions, recommendations, and findings. It also shows whether the objectives of the research and hypothesis have been fulfilled.

5.2 Findings

5.2.1 Status of the Courts in Determination of what is Reasonable and Necessary.

The Kenya Data Protection Act establishes a foundational framework for data retention management in the country. However, Section 39's vague requirement that data be retained for only as long as is "reasonable and necessary" poses substantial challenges for Data Controllers and Data Processors. The absence of clear guidelines results in inconsistent practices, potentially leading to extended data retention periods, heightened risks of unauthorized access, data misuse, and breaches. These risks have profound implications, affecting not only individuals' privacy and security but also organizations' compliance, reputation, and overall data governance.

5.2.2 The Application of clear justification for data retention periods through different Parameters in Germany

In Germany, data protection is rigorously enforced through the Federal Data Protection Act (BDSG), which aligns closely with the European General Data Protection Regulation (GDPR). The BDSG emphasizes the principle of data minimization, requiring clear justification for data retention periods. German companies prioritize meticulous documentation of data processing activities to ensure compliance with necessity and proportionality principles. This involves detailed data flow analyses and retention impact evaluations, engaging legal, technical, and operational teams to maintain transparency and accountability.

5.2.3 Possibility of the courts in Kenya Adopting German-Inspired Retention and Disposal Practices.

The assessment done in chapter four demonstrates and affirms the possibility of the courts in Kenya adopting Germany's structured approach to data retention by integrating clear categorization frameworks and evidence-based retention practices into judicial interpretations of Kenya's Data Protection Act (DPA).

5.3 Recommendations

5.3.1 Need for reliance on scholarly works on Data Protection by the Courts in Data Retention Practices.

Courts must increasingly rely on scholarly works to navigate the complexities of data retention practices, particularly where statutory frameworks lack specificity. Academic research provides critical insights into balancing privacy rights with organizational needs, such as defining "reasonable" retention periods under principles like the GDPR's storage limitation. For instance, scholarly analyses of Germany's Federal Data Protection Act (BDSG) and the European Court of Justice's proportionality standards offer models for reconciling indefinite retention risks with public interest exemptions for research. Studies also highlight the importance of data minimization and purpose specification, as seen in institutional policies like the University of Oxford's three-year minimum retention period for research data, which aligns with GDPR exceptions for anonymized archival use. By integrating academic frameworks such as categorizing data by sensitivity, enforcing secure disposal protocols, and mandating multi-stakeholder audits—courts can address ambiguities in laws like Kenya's Data Protection Act. Scholarly works further emphasize the role of transparency in retention policies, ensuring individuals understand how their data is managed, a principle underscored by GDPR's fairness requirements. This interdisciplinary approach enables courts to harmonize legal standards with evolving technological and ethical demands, fostering consistency in data governance globally.

5.3.2 Need for reliance on judicial precedent.

The reliance on judicial precedent is crucial in shaping data retention practices, as it provides a consistent and predictable framework for interpreting ambiguous legal provisions. Judicial decisions, particularly those from jurisdictions like Germany and the European Court of Justice, offer valuable guidance on balancing privacy rights with organizational needs. By referencing precedents such as the ECJ's rulings on proportionality and necessity in data retention, courts can clarify the meaning of terms like "reasonable and necessary" in laws like Kenya's Data Protection Act. This approach ensures that data handling practices align with established legal standards, reducing inconsistencies and enhancing accountability in data governance.

5.3.3 Need for use of Data Protection expert witnesses

The use of data protection expert witnesses is essential in legal proceedings involving data retention practices. These experts provide critical insights into complex data protection issues, helping courts understand whether organizations have implemented adequate security measures and complied with relevant regulations like the GDPR. Expert witnesses can analyze data breaches, assess the effectiveness of data protection policies, and determine liability in cases of unauthorized access or misuse. Their specialized knowledge is crucial for establishing the extent of harm caused by breaches and for guiding courts in making informed decisions about data protection standards. By leveraging expert testimony, courts can ensure that data handling practices align with legal requirements, enhancing accountability and compliance in data governance

5.4 Conclusion

This study has achieved all its objectives as set out in Chapter One. Moreso, it has proved its hypothesis in light of its findings. The following were the objectives;

1. Examine the risks of indefinite data retention and the need for clear guidelines to ensure effective data protection.
2. Analyze Germany's jurisdictional framework regarding data retention practices, focusing on the compatibility of its laws with EU regulations and the European Court of Justice rulings on national data retention policies.
3. Propose Clear Guidelines by comparing with other jurisdictions like Germany, which has specific data retention laws under Germany's regulations.

5.4.1 Objective i

This objective has examined the risks associated with indefinite data retention and highlighted the necessity for clear guidelines to ensure effective data protection. Through a comprehensive analysis, the study has identified the challenges posed by ambiguous data retention practices, such as increased risks of unauthorized access, data misuse, and breaches.

5.4.2 Objective ii

This objective has analyzed Germany’s jurisdictional framework for data retention and its alignment with EU regulations, particularly through the lens of European Court of Justice (ECJ) rulings.

5.4.3 Objective iii

This study has successfully achieved its research objective by proposing actionable guidelines for data retention through a comparative analysis of Germany's structured legal framework under the Federal Data Protection Act (BDSG) and Telecommunications Act (TKG). By examining Germany's approach which mandates data categorization such as strict safeguards for sensitive data like IP addresses under the Hesse draft law, time-bound retention schedules such as 4–10 weeks for telecom data, revised to one month for IP storage, and judicial oversight reinforced by European Court of Justice (ECJ) ruling the study identifies replicable strategies for balancing security and privacy.

5.4.5 Hypothesis

This study has validated its hypothesis by demonstrating that Section 39 of Kenya's Data Protection Act (DPA), which permits indefinite data retention under the "reasonably necessary" standard, creates systemic risks due to inconsistent interpretations among Data Controllers and Processors. The research revealed that while the DPA's General Regulations recommend retention schedules, the absence of prescribed time limits in the Act itself leads to fragmented practices, such as prolonged storage of sensitive data without standardized deletion protocols. By analyzing breach risks linked to over-retention such as unauthorized access and misuse highlighted in Kenya's cybersecurity obligations the study confirmed that vague retention policies erode public trust and complicate compliance. Comparisons with Germany's framework, which mandates time-bound retention such as 4–10 weeks for telecom data and judicial oversight, underscored the efficacy of specific guidelines in mitigating risks. The findings advocate for aligning Kenya's DPA with GDPR-inspired storage limitation principles, such as defining purpose-specific retention periods and enforcing cryptographic erasure, to reduce variability, enhance accountability, and strengthen data security.

BIBLIOGRAPHY

Books

Bygrave L A, 'International Data Privacy Codes' in Bygrave L A (ed) *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014.

Graham Greenleaf, *Data Protection and Privacy: A Global Perspective,* 2017.

Harris S, Cybersecurity: A Comprehensive Guide to Information Security, *McGraw-Hill Education,* New York, 2015.

Beauchamp T L and Childress J F, *Principles of Biomedical Ethics,* 7th ed., Oxford University Press, New York, 2012.

Conference Papers

Urban T, Tatang D, Degeling M, Holz T, and Pohlmann N, 'A study on subject data access in online advertising after the GDPR' ESORICS 2019 International Workshops, Luxembourg, September 26–27, 2019.

Hard copy Journal Articles

Kuehn B M, 'Groups Experiment with Digital Tools for Patient Consent' 310 *Journal of the American Medical Association* 7, 2013.

Moor J, 'The Ethics of Privacy Protection' 39 *Library Trends* 1–2, 1990.

Moor J, 'Towards a theory of privacy in the information age' 27 *ACM SIGCAS Computers and Society* 3, 1997.

Tavani H, 'Philosophical theories of privacy: Implications for an adequate online privacy policy' 38 *Metaphilosophy* 1, 2007.

Journal Articles

Ayalew Y E, 'Untrodden paths towards the right to privacy in the digital era' *International Data Privacy Law,* 2022, 16–32 - https://doi.org/10.1093/idpl/ipab031, 2022.

Bardosh K, Murray M, Khaemba AM, Smillie K, and Lester R, 'Operationalizing Health to improve patient care: A Qualitative Implementation Science Evaluation of the WelTel Texting Intervention in Canada and Kenya' *Globalization and Health,* 2017, 1-15 – https://globalizationandhealth.biomedcentral.com/articles/10.1186/s12992-017-0271-5, 2017.

Brkan M, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' International Journal of Law and Information Technology, 2019, 91-121 – https://doi.org/10.1093/ijlit/eaz006, 2019.

Clifford D, Graef I, and Valckl P, 'Pre-formulated declarations of data subject consent citizen-consumer empowerment and the alignment of data, consumer and competition law protections' German Law Journal, 2019, 679-721 – https://www.cambridge.org/core/journals/german-law-journal/article/preformulated-declarations-of-data-subject-consent-citizenconsumer-empowerment-and-the-alignment-of-data-consumer-and-competition-law-protections/ 2019.

Connolly L, Wall D S, Lang M, and Oddson B, 'An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability' Journal of Cybersecurity, 2020 - https://doi.org/10.1093/cybsec/tyaa009 , 2020.

Christopher G. Bradley, 'Privacy for Sale: The Law of Transactions in Consumers' Private Data' Yale Journal on Regulation, 2023, 127-212, https://openyls.law.yale.edu/bitstream/handle/20.500.13051/18236/Christopher%20G.%20Bradley%20Privacy%20for%20Sale%20The%20Law%20of%20Transactions%20in%20Consumers%20Private%20Data%2040%20Yale%20J.%20on%20Regul.%20127%20(2023).pdf?sequence=1&isAllowed=y[1]

Goldfarb A and Tucker C, 'Privacy and Innovation' 12 Innovation Policy and the Economy 1, 2012.

Hintze M, 'Viewing the GDPR through a de-identification lens: A tool for compliance, clarification, and consistency' International Data Privacy Law, 2018, 1-22 – https://ssrn.com/abstract=2909121 , 2018.

Hoffmann W, Latza U, Baumeister SE, Brünger M, Buttmann-Schweiger N, Hardt J, and Hoffmann V, 'Guidelines and recommendations for ensuring Good Epidemiological Practice (GEP)' European Journal of Epidemiology, 2019, 301-317 – https://www.researchgate.net/publication/331500563_Guidelines_and_recommendations_for_ensuring_Good_Epidemiological_Practice_GEP_a_guideline_developed_by_the_German_Society_for_Epidemiology, 2019.

Holm S and Ploug T, 'Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research' 30 Bioethics 9, 2016.

Inau ET, Nalugala R, Nandwa WM, Obwanda F, Wachira A, and Cartaxo A, 'Fair Equivalency, Regulatory Framework and Adoption Potential of Fair Guidelines in health in Kenya' Data Intelligence, 2022, 853 – 862 https://direct.mit.edu/dint/article/4/1/162/109905/Fair-Equivalency-Regulatory-Framework, 2022.

Podkowik J, Rybski R, and Zubik M, 'Judicial dialogue on data retention laws: A breakthrough for European constitutional courts' International Journal of Constitutional Law, 2021, 1597-1631 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4637947, 2021.

Koeva M, Stöcker C, Crommelinck S, Ho S, Chipofya M, Sahib J, and Bennett R, 'Innovative remote sensing methodologies for Kenyan land tenure mapping' Remote Sensing, 2020, 1-27 https://www.mdpi.com/2072-4292/12/2/273, 17 January 2020.

Makulilo, Alex B 'Privacy in mobile money: Central banks in Africa and their regulatory limits,' *International Journal of Law and Information Technology* 23, 2015.

Maseh E, 'Managing court records in Kenya' 25 *African Journal of Library,* Archives & Information Science, 2015.

Mugambi M, 'Data Protection Compliance in Kenya: Evaluating the New Regulatory Landscape' *Journal of Data Protection and Privacy,* 2021, 131–145 - https://www.henrystewartpublications.com/jdpp/v4 2021.

Mutua SN, and Zhang Y, 'Online content regulation policy in Kenya; Potential challenges and possible solutions' *Journal of Cyber Policy,* 2021, 177-195 – https://doi.org.ezproxy.library.strathmore.edu/10.1080/23738871.2021.1916974, published 2021.

Odhiambo, E 'Privacy and Data Protection in Kenya; Evaluating the Implementation of the Data Protection Act'. *East African Law Journal.*

Riofrio J, 'The Natural Law Formula and the Missing Link: Tracing and Updating Aquinas' Methodology' *Forum Prawnicze*, 2022, https://ssrn.com/abstract=4439018, on December 1, 2022.

Rojszczak M, 'National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts' European Constitutional Law Review, 2021, 607-635, https://doi.org/10.1017/S1574019621000353, 2021

Rustad ML and Koenig TH, 'Towards a global data privacy standard' Florida Law Review, 2019, 366- 453 https://www.floridalawreview.com/towards-a-global-data-privacy-standard 2019.

Veale M, Binns R, and Ausloos J, 'When data protection by design and data subject rights clash' *International Data Privacy Law*, 2018, 1-19 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081069 2018.

Wachter S and Mittelstadt B, 'A right to reasonable inferences: re-thinking data protection law in the age of big data AI' *Columbia Business Law Review,* 2019, – https://journals.library.columbia.edu/index.php/CBLR/article/view/1234, 2019.

Newspapers

Gordon S and Ram A, 'Information wars: How Europe became the world's data police' Financial Times, 2018, https://www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8 on 20 May, 2018.

Reports

Media Council of Kenya, Data Governance Guide For Media Practice in Kenya, October 2023.

Research Papers

Ayalew Y E, 'Untrodden paths towards the right to privacy in the digital era' International Data Privacy Law, 2022, 2-41 - https://doi.org/10.1093/idpl/ipab031, 2022.

Custers B, 'The Power of Knowledge: Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology', Tilburg University, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3186639, 2016.

Goddard M, 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' International Journal of Market Research, 201, 703–705 - https://doi.org/10.2501/IJMR-2013-060, 2013.

Kitili J and Abiero D, 'Kenya's Digital Infrastructure Under Threat; A Look at Anonymous Sudan's Thwarted Cyber Attack Attempt and its Implications for Kenya's Digital Systems' Centre for Intellectual Property and Information Technology Law, 2023, https://cipit.strathmore.edu/kenyas-digital-infrastructure-under-threat-a-look-at-anonymous-sudans-thwarted-cyber-attack-attempt-and-its-implications-for-kenyas-digital-systems/, August 2023.

Medi M, 'Online Surveillance and Freedom of Expression in Kenya' University of Nairobi, Thesis, 2021, -http://erepository.uonbi.ac.ke/handle/11295/161037, 2021.

Mugo E W, 'Governance in the Data Age: Application of Corporate Governance to Ensure Consumer Data Protection in Kenya' University of Nairobi, Thesis, 2018, 22-97 https://erepository.uonbi.ac.ke/handle/11295/108799 , 2018

Mukuki, Allan, and Alex Assenga. 'Comparative study of data protection legislation frameworks across the East African community', 2024.

Nyaga, Bernard M, Joy Cheruto Ondego, and Mogesi Joel, 'Mediation and Data Protection Law in Kenya: Appraising ADR for Optimal Access to Justice under the DPA 2019', 2023.
Nyawara D O, 'Regulation of Fintech: Analysis of data protection provisions aimed at protecting consumers in Kenya' Strathmore University, Thesis, 2021, 34-79, http://hdl.handle.net/11071/12930 2021.

Oyatsi T R, 'Balancing competing interests: A study on Kenya's Ability to reconcile national security with the right to privacy' Strathmore University, Thesis, 2017 1-51 https://su-plus.strathmore.edu/handle/11071/5590, 2017.

Sartor G and Lagioia F, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' European Parliament, Panel for the Future of Science and Technology (STOA), Study No. PE 641.530, 2020, 1–84 – https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN, April 2020.

Schade J, 'Kenya "Olkaria IV" Case Study Report; Human Rights Analysis of the Resettlement Process' Centre on Migration, Citizenship and Development (COMCAD), Working Paper Number 51, 2017, 1-171 https://www.ssoar.info/ssoar/bitstream/handle/document/51409/ssoar-2017-schade-Kenya_Olkaria_IV_Case_Study.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2017-schade-Kenya_Olkaria_IV_Case_Study.pdf, 2017.

Solove D J, 'A Taxonomy of Privacy' University of Pennsylvania Law Review, 2006, 477–560, https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/, January, 2006.

Yusuf B, 'Harmonization of Data Governance Frameworks in Africa' Centre for International Governance Innovation, Digital Policy Hub, 2024, 1-7 https://www.cigionline.org/documents/3133/DPH-paper-Yusuf_3HvhA8r.pdf, April, 2024.

VT OMNES
VNVM SINT