Privacy and personal data protection in Africa

A rights-based survey of legislation in eight countries

Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries

Coordination team
Koliwe Majama (APC)
Janny Montinat (APC)
Anriette Esterhuysen (APC)

Compiled by
Hlengiwe Dube, University of Pretoria, Centre for Human Rights
Avani Singh, ALT Advisory

Copy editing and proofreading
Lynne Stuart (Idea in a Forest)
Lori Nordstrom (APC)
Lynn Welburn

Publication production and support
Cathy Chen (APC)

Graphic design
Monocromo

Published by the African Declaration on Internet Rights and Freedoms Coalition
https://africaninternetrights.org
May 2021

ISBN 978-92-95113-39-8
APC-202103-CIPP-T-EN-DIGITAL-329
Supported by the Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH

Table of contents

Abbreviations and acronyms

ACHPR	African Commission on Human and Peoples' Rights
AfCTFA	African Continental Free Trade Area
AfDec	African Declaration on Internet Rights and Freedoms
AU	African Union
ccTLD	Country code top-level domain
CSO	Civil society organisation
DPA	Data protection authority
EAC	East African Community
ECOWAS	Economic Community of West Africa States
GDPR	General Data Protection Regulation
HRBA	Human rights-based approach
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communications technology
ISP	Internet service provider
SADC	Southern African Development Community
SDGs	Sustainable Development Goals
UDHR	Universal Declaration of Human Rights
UNHRC	United Nations Human Rights Committee
UPR	Universal Periodic Review

Please note that these are the abbreviations and acronyms most frequently used throughout this publication. This list is not exhaustive, as there are also numerous country-specific abbreviations and acronyms that are only used in the chapters from those particular countries.

Kenya

Sigi Waigumo Mwanzia[1]

Executive summary

Kenya's legislative data protection framework, the Data Protection Act (DPA) of 2019, and practice are still in their nascent stages. This offers many opportunities and challenges to promote the entrenchment of best practices in the data protection and privacy arena and to advocate for the simultaneous application of the human rights-based approach framework as outlined in the report below.

Since 2007, various stakeholders including civil society organisations (CSOs), private sector entities and international organisations, amongst others, have been at the forefront of advocating for a comprehensive information privacy framework.

1 The author would like to express appreciation to Ben Roberts (Liquid Telecom), Mercy Mutemi (Nzili and Sumbi Advocates), Grace Bomu (Centre for Intellectual Property and Information Technology Law, Strathmore University) and Gloria Madegwa and Esban Muthoni (Defenders Coalition) who participated in the interviews that supplemented and enriched this country report with multistakeholder perspectives.

In recent times, these advocacy efforts have involved the filing of judicial petitions seeking the implementation of constitutional provisions on privacy and data protection, strengthening of the provisions of the DPA, prevention of the abuse of state powers and/or the infringement of privacy rights by the national government and its agencies during the COVID-19 pandemic, among others.

This report notes that the main challenge in Kenya's data protection and privacy sphere includes a reluctance and failure to internalise and implement the provisions of the DPA by both state and non-state actors, nearly a year after the framework was enacted in November 2019. This will be a key issue for the data protection (regulatory) authority tasked with overseeing the implementation of the DPA, which the government is in the process of establishing.

This report is intended for African Declaration on Internet Rights and Freedoms (AfDec) Coalition members, regional bodies, national human rights institutions, data protection authorities, digital rights activists, CSOs, media rights journalists and bloggers concerned with human rights and internet governance.

Methodology

This country report was generated using primary information received from Kenya-based partners (individuals and organisations), and secondary information sourced online.

The primary information was collected via semi-structured interviews using a set of carefully tailored questions which were specific to each interviewee, as well as general questions addressed to the entire group. These questions sought the interviewee's

individual and organisational perceptions about Kenya's data protection and privacy sphere, including the DPA's enactment process, implementation challenges and opportunities noted so far. The interviewees were selected according to commonly-recognised stakeholder groupings, and included the government, CSOs, academia, private sector and the technical community, as well as sectoral expertise at the policy, technology, human rights, research and legal levels. The interviewees were selected using random (stratified) sampling and interviews were all conducted using a secure teleconferencing platform, namely Zoom.

The secondary information was collected via online desk research which was restricted to the 2007 to 2020 period, given the significance of this timeline for the data protection (legislative) process. This information included the Constitution of Kenya, 2010, the DPA, 2019 and other relevant administrative, policy, regulatory and legislative documents, international and regional material (treaties, instruments, standards, review processes), litigation material from national courts (pleadings and determinations), research reports and other assessments expounding on Kenya's political, economic, social and rights context for purposes of the DPA, 2019.

Country context

The period from 2007 to 2020 in Kenya was characterised by significant social, political and economic advancements and changes. These triple indicators of developmental progress have all been affected by shocks occasioned by the COVID-19 global pandemic.

Kenya's development blueprint, Vision 2030, was launched in 2008 and encapsulates Kenya's broad economic, social and

political strategies.[2] This developmental blueprint is being implemented in stages through five-year medium-term plans and complements Kenya's commitments under the Sustainable Development Goals (SDGs)[3] and the African Union Agenda 2063.[4]

Politically, the Constitution of Kenya (2010) provides for the transformative interpretation and application of civil, political, economic, social and cultural rights across all 47 counties in the Republic of Kenya. This transformative potential is further encapsulated in the Bill of Rights which contains numerous human-rights (including internet-related rights) guarantees which are indicative of Kenya's firm commitment to the human rights-based approach, at least at the theoretical level.

The Constitution of Kenya, 2010 was promulgated following mass calls for democratic reforms, pluralism, ceasure of the presidency's dominance and the state's practice of secrecy and information controls. These calls were also heavily influenced by the effects of the 2007 elections and post-election violence,[5] which was itself symptomatic of systemic post-independence challenges. These challenges – most of which persist to date – included economic disparities,[6] governance failures, mass corruption, land grievances, and the "political manipulation of ethnic tensions,"[7] amongst others. All these challenges led to a desire and strong push for "the second liberation."[8]

2 https://vision2030.go.ke/

3 https://sustainabledevelopment.un.org/memberstates/kenya

4 https://au.int/en/agenda2063/overview

5 This election, and the processes which arose subsequently, were marred by electoral irregularities, violence and the politicisation of international criminal processes.

6 Brownsell, J. (2013, 3 March). Kenya: What went wrong in 2007? *Al Jazeera*. https://www.aljazeera.com/features/2013/3/3/kenya-what-went-wrong-in-2007

7 Human Rights Watch. (2008, 16 March). Ballots to Bullets: Organized Political Violence and Kenya's Crisis of Governance. https://www.hrw.org/report/2008/03/16/ballots-bullets/organized-political-violence-and-kenyas-crisis-governance

8 Interview with Grace Mutung'u, research fellow at the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, 12 October 2020.

On the socioeconomic front, Kenya maintained her position as "one of the fastest growing economies in Sub-Saharan Africa"[9] in 2019. Despite this, the country's burgeoning public debt (external and domestic) rose from KSH 5,607.91 billion (USD 51.523 billion) in May 2019 to KSH 6,282.82 billion (USD 57.718 billion) in May 2020.[10] This has further been met by challenges of a fluctuating currency[11] and dwindling foreign exchange reserves.[12] These challenges continue to affect Kenya's social environment, as well as fledgling "green economy" and "smart city" drives.

Kenya continues to promote and protect internet-related human rights through its Bill of Rights and via the extensive expansion of the nation's information, technology and communications (ICT) policy and legislative frameworks. Secondly, Kenya has invested heavily, either through state-sponsored initiatives or public-private partnerships, in ICT infrastructure which continues to promote individuals' ability to access and use digital platforms and communication technologies. ICT policy making, and in some instances, regulatory powers, continue to be relegated to either the ICT Ministry, the National Communications Secretariat[13] or the Communications Authority of Kenya, which all have divergent mandates. On the other hand, legislative powers rest exclusively with Kenya's bicameral legislature, which has enacted numerous frameworks promoting the protection of internet-related human rights.

9 https://www.worldbank.org/en/country/kenya/overview

10 Central Bank of Kenya. (2020). *Monthly Economic Indicators, May 2020*. http://www.centralbank.go.ke/monthly-economic-indicators

11 Guguyu, O., & Ambani, B. (2020, 23 September). Central Bank loses grip on the Kenyan shilling. *Nation.* https://nation.africa/kenya/business/cbk-loses-grip-on-the-kenyan-shilling-2305786

12 Omondi, D. (2020, 29 March). CBK boss goes all out to protect Shilling. *The Standard.* https://www.standardmedia.co.ke/business/article/2001366051/cbk-boss-goes-all-out-to-protect-shilling

13 The NCS is tasked with "advising the Government on the adoption of a communication policy" under section 84 of the Kenya Information and Communications Act. (1998). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%201998

The establishment of a data protection framework in Kenya has been driven and stalled by numerous incentives and barriers. Economic and trade considerations, following the imposition of extraterritorial responsibilities located in the GDPR and Kenya's desire to retain her "competitive edge" against African countries with established data protection frameworks, shaped the government's priorities and reinforced political will.[14] Crucially, these considerations were solidified following Kenya's voluntary championing of the "digital economy" agenda,[15] as part of her Smart Africa Alliance membership.[16] It is crucial to note that these twin considerations shattered the government's initial legislative reluctance, and watered down the perception that a framework would erect barriers affecting the government's previously unchecked collection and processing of individuals' personal data for numerous agendas, including the registration of persons.

Conversely, civil society organisations "strengthened their coordination efforts"[17] and solidified their calls for the legislative framework following two fundamental events: the data-driven 2017 election – and the petition which was subsequently lodged – and the government's introduction of digital identity drives in 2019. Private sector actors and the technical internet community were largely motivated by the desire to maintain their competitive edge, in an increasingly consumer-aware and privacy-hungry market.

Multiple stakeholders from different sectors continue to impact and shape Kenya's personal data protection landscape, and either influence or retard the entrenchment of a human rights-based

14 Interviews with Grace Mutung'u, research fellow at the Centre for Intellectual Property and Information Technology Law, Strathmore University, 12 October 2020 and John Walubengo, lecturer and member of the National Taskforce on Blockchain & AI, 10 October 2020.

15 ICT Ministry. (2019). *Digital Economy Blueprint.* https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf

16 https://smartafrica.org

17 Interview with Grace Mutung'u, 12 October 2020. Op. cit.

approach to data protection. These include, but are not limited to, members of the public,[18] state agencies,[19] civil society organisations,[20] constitutional commissions,[21] private sector entities (including those without a physical presence in Kenya)[22] and academics.[23]

Constitutional underpinning

The right to privacy and data protection is explicitly guaranteed under Article 31, Constitution of Kenya, 2010. This right is limited and derogable, subject to the legality, necessity and proportionality limbs under Article 24, and provides as follows:

> Every person has the right to privacy, which includes the right not to have:
>
> - their person, home or property searched
> - their possessions seized
> - information relating to their family or private affairs unnecessarily required or revealed
> - the privacy of their communications infringed.

18 These include, but are not limited to, Abraham M. Kilonzo (ICT personnel), Alex Gakuru (technology rights defender), Michael Gitagia, Mugambi Laibuta (trained mediator and policy and legislative drafting professional), Nicholas Kanyagia, Mark Tum, and Peter Muya (ICT consultant). See the Communications Authority of Kenya's "Published Findings": https://ca.go.ke/consumers/public-consultations/published-findings

19 These include, but are not limited to, the ODPC, the ICT Ministry, the CA, the CAK, the National Cohesion and Integration Commission, the National Security Advisory Committee. During the taskforce deliberations (2018), external state agencies from the United States provided comments, including the US Department of Commerce's International Trade Administration and the US Chamber of Commerce. Ibid.

20 These include, but are not limited to, Amnesty International Kenya, ARTICLE 19, the Kenya ICT Action Network, the National Coalition of Human Rights Defenders (Kenya), Privacy International, Research ICT Africa, and FSD Kenya, between 2018 and 2019. Ibid.

21 These include, but are not limited to, the KNCHR and the CAJ. Ibid.

22 These include, but are not limited to, Google Kenya, Facebook, Technology Service Providers of Kenya, CODE-IP, the Kenya Private Sector Alliance, Mozilla, Amazon Web Services, Airtel, GSMA, IBM, KENIC, Microsoft, MultiChoice Kenya, Safaricom PLC, Savannah Training Solution Limited, Seven Seas Technologies Group, the Foschini Group Kenya Limited, Uber East Africa, AIG Kenya Insurance Company Ltd, Allan Gray Kenya Limited, ATLANCIS Technologies, Branch International Limited, InVenture Mobile Limited (Tala), KCB Bank Kenya, Mastercard, M-Kopa Solar, between 2018 and 2019. Crucially, law firms also actively submitted comments during the 2018-2019 processes. Ibid.

23 This includes, but is not limited to, the Centre for Intellectual Property and Information Technology Law.

Crucially, Article 19 (2) reiterates that the "purpose of recognising and protecting human rights and fundamental freedoms is to preserve the dignity of individuals and communities and to promote social justice and the realisation of the potential of all human beings."

The judiciary continues to interpret this right, as far back as 2007 and as recently as 2020, with most cases being raised against mass or closely-affiliated data controllers and processors including the state, private entities and individuals. These have been centred on issues affecting human dignity generally; inter-sex persons in prison;[24] privacy rights accruing to state corporations and third parties in the context of illegally-obtained information with a public interest;[25] waiving of consent during warrantless search-and-seizure investigations by the national police service[26] and the use of (thin SIM) technology;[27] the distribution of private photographs;[28] the installation of the device management system with alleged capabilities to interfere with private communications;[29] search-and-seizure of data stored on a computer system without mandatory judicial oversight;[30] Kenya Revenue Authority's sourcing of tax information, including from third parties, without warrants;[31] and the privacy risks latent in Kenya's digital ID system (NIIMS),[32] amongst others.

24 *R.M v Attorney General & 4 others* [2010] eKLR. http://kenyalaw.org/caselaw/cases/view/72818

25 *Okiya Omtatah Okoiti & 2 others v Attorney General & 3 others* [2014] eKLR. http://kenyalaw.org/caselaw/cases/view/103808

26 *Samson Mumo Mutinda v Inspector General National Police Service & 4 others* [2014] eKLR. http://kenyalaw.org/caselaw/cases/view/94430

27 *Bernard Murage v Fineserve Africa Limited & 3 others* [2015] eKLR. http://kenyalaw.org/caselaw/cases/view/109772

28 *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* [2016] eKLR. http://kenyalaw.org/caselaw/cases/view/129282

29 *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/193383/

30 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/191276/

31 *Okiya Omtatah Okoiti v Attorney General & another* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/191427/

32 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/189189/

Notably, Kenyan courts took notice of the lack of a comprehensive legislative framework but refrained from exercising judicial discretion given the existence of the "separation of the powers" principle in the constitution. Instrumentally, the High Court in the latter case took judicial notice of the DPA, 2019 and issued two crucial statements: the need for an "effective implementation and enforcement" of the DPA, 2019, and the existence of various "gaps" in the framework with implications for children. These judgments continue to have varying effects on the protection of personal data and privacy, and the implementation of the human rights-based approach in Kenya.

Existence of other laws dealing with privacy and data protection online

Kenya's legislative arena is laden with frameworks containing insufficient offline and online privacy and data protection provisions. These include the National Payment System Act (2011),[33] the Consumer Protection Act (2012),[34] amendments to the KICA, 1998 and its regulations, including the Consumer Protection Regulations (2010) and the Registration of SIM Cards Regulations (2015).

Additionally, the Access to Information Act (ATI Act) (2016)[35] contains various data protection provisions, and empowers the CAJ with dual data protection and access to information powers. As noted above, this linkage was part of drives to push for "the second liberation", where stakeholders recognised and affirmed the mutually-reinforcing nature of the right to privacy and

33 http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2039%20of%202011

34 Section 2, Consumer Protection Act (2012) defines personal information as "information other than credit information about a consumer's character, reputation, health, physical or personal characteristics or mode of living or about any other matter concerning the consumer." http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2046%20of%202012

35 Section 21 (1) (a to h), Access to Information Act (2016). http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016

data protection and access to information. Despite this, these provisions do not offer comprehensive guarantees protecting the right to privacy and data protection, and the CAJ has not allocated the same amount of resources to the data protection components of its mandate.

While Articles 31 and 33, Constitution of Kenya, 2010 are interpreted as promoting the right to digital anonymity and "pseudonymous expression",[36] mandatory SIM card registration drives by the Kenyan government have watered down these protections. Despite Kenya avoiding the implementation of "real-name policies", as proposed in the KICA (Amendment) Bill, 2019,[37] and refraining from barring the use of anonymity tools in legislative frameworks, the "unauthorised interference" provision in the Computer Misuse and Cybercrimes Act (2018) affects encryption rights. As ARTICLE 19 noted in its 2015 report, "encryption rights are crucial for various stakeholders, including human rights defenders, whistleblowers, journalists and activists who are often the subject of surveillance by intelligence or law enforcement agencies."[38]

Regional and international commitments on privacy and personal data protection

Kenya, by virtue of Articles 2(5) and (6), Constitution of Kenya, 2010, recognises that the "general rules of international law shall form part of the law of Kenya" and that "any treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution." By virtue of international law and these constitutional provisions, Kenya is bound to numerous regional and international commitments on privacy and data protection.

36 Monteiro, A. (2014, 13 June). Access intervenes at ECtHR for the right to be anonymous online. *Access Now*. https://www.accessnow.org/access-intervenes-at-ecthr-for-the-right-to-be-anonymous-online

37 http://kenyalaw.org/kl/index.php?id=9091

38 ARTICLE 19. (2015). *Right to Online Anonymity.* https://www.article19.org/resources/report-the-right-to-online-anonymity

At the regional (AU) level, Kenya's data protection and privacy responsibilities can be inferred under various provisions, including Articles 4 to 6, of the African Charter which guarantee the "inviolability of the human being," "human dignity" and individual "liberty and security". The continued failure to insert an explicit right to privacy in the African Charter has resulted in numerous countries, including Kenya, being "implicitly bound" under other instruments, including the ACERWC, 1990, which Kenya ratified and deposited in 2000.[39]

Kenya is one of 44 AU member states which have not ratified the AU Convention. However, in 2018, Kenya's ratification of the region's free trade agreement, the AfCFTA, imbued the state with privacy and data protection responsibilities. Article 15 (a)(ii), AfCFTA provides that states must take measures to ensure "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[40]

Furthermore, Kenya stands guided by Principles 40 and 41 of the ACHPR Declaration due to its soft law status which maintains that "everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information" and protections from both targeted and mass surveillance.[41] Kenya also stands guided by the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa[42] which recognised that "privacy online is

39 ACERWC. (2020). *Ratifications Table*. https://www.acerwc.africa/ratifications-table/

40 The Africa Union. (2018). *Agreement Establishing the African Continental Free Trade Area*. https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area

41 African Commission on Human and Peoples' Rights. (2019). *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019.* https://www.achpr.org/legalinstruments/detail?id=69

42 ACHPR. (2017) *Recommendations and Resolutions Adopted by the African Commission on Human and Peoples' Rights - ACHPR/Res. 362(LIX) 2016: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa*. https://www.achpr.org/adoptedresolution

important for the realisation of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."

At the sub-regional (EAC) level, the heads of states continue to withhold their assent to the EAC Human and Peoples' Rights Bill (2011), which would have provided the peoples of the sub-region, including Kenya, with an explicit (sub-regional) right to privacy under Article 19 of this bill.[43] Out of the six EAC member states, Kenya surprisingly failed to offer its usual sub-regional leadership on the legislative front, following Uganda's enactment of its data protection framework in February 2019 as well as Rwanda's ratification of the AU Convention in October 2019, before Kenya enacted her own data protection framework in November 2019.

Internationally, Kenya is bound by Article 17, ICCPR which guarantees individuals' right to privacy (over their) "family, home or correspondence." Positively, Kenya reaffirmed its commitment to the promotion of internet freedom, including the right to privacy online, through its Freedom Online Coalition membership.[44] The Republic of Kenya pledged, in conjunction with multiple stakeholders, to "adopt and encourage policies and practices, nationally and internationally, that promote the protection of human rights and fundamental freedoms online."[45]

Lastly, despite efforts by the Council of Europe (Data Protection Unit), to convince various states, including Kenya, to accede to and integrate the "international standards as enshrined

43 Greenleaf, G., & Cottier, B. (2020). *Comparing African Data Privacy Laws: International, African and Regional Commitments*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478

44 https://freedomonlinecoalition.com/about-us/members

45 Freedom Online Coalition. (2014). *The Tallinn Agenda - Recommendations for Freedom Online*. https://freedomonlinecoalition.com/underpinning-documents

in Convention 108+,"[46] Kenya is still one of the many non-EU member states which have not yet ratified Convention 108.[47]

Existence of a comprehensive data protection law

Kenya's Data Protection Act, 2019 (DPA) received presidential assent on 8 November 2019 and came into force shortly thereafter on 25 November 2019. The decision to formalise the data protection process commenced, at least for some stakeholders, in 2007, following calls for the "second liberation", and the desire for democratic, right-respecting, transparent and accountable processes and institutions in Kenya.

Between 2016 and 2018, civil society organisations working or interested in information rights (including the right to access information, expression and privacy under Articles 31, 33 and 25, Constitution of Kenya, 2010) converged efforts, resources and interests. This convergence witnessed the successful enactment of an information access legislation, i.e., the ATI Act, 2016, and led to a diversion of their calls for an exclusive informational privacy legislative framework.

These calls were formally responded to by the ICT Ministry, following its constitution of the "Taskforce on the Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya."[48] This task force prepared the Privacy and Data Protection Policy 2018[49] and the Data Protection Bill

46 Council of Europe. (2018, 2 October). Data Protection Unit provides support to the Kenyan authorities in drafting legislation on protection of privacy and personal data. https://www.coe.int/en/web/data-protection/-/data-protection-unit-provides-support-to-the-kenyan-authorities-in-drafting-legislation-on-protection-of-privacy-and-personal-data

47 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Reference, ETS No.108. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

48 The Kenya Gazette. (2018). *Gazette Notice No. 4367, Vol. CXX - No. 56.* http://kenyalaw.org/kenya_gazette/gazette/volume/MTcwNg--/Vol.CXX-No.56

49 Ministry of ICT. (2018). *Privacy and Data Protection Policy 2018*. http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf

A BRIEF HISTORY OF
DATA PROTECTION IN KENYA

2007

2007 elections and calls for **"the second liberation."**

2009

The **Data Protection Bill (2009**) is released by the ICT Ministry.

2010

Kenya promulgates the **2010 Constitution of Kenya**. Article 31 explicitly protects the right to privacy and data protection.

2011

The **Data Protection Bill, 2009** is received and considered by the Commission for the Implementation of the Constitution. Stakeholder consultations are held in 2012.

2013

The **Data Protection Bill, 2013** is released by the ICT Ministry.

2016

The **Access to Information Act, 2016** is enacted. Under section 21, CAJ possesses dual access to information and data protection powers.

2018

Data Protection Taskforce releases the Privacy and Data Protection Policy & the Data Protection Bill (2018). Public consultations are held.

2018

The **Data Protection Bill, 2018** is tabled before the Senate in May 2018.

2019

The **Data Protection Bill, 2019** is passed by the National Assembly, the President assents the Data Protection Act, 2019 on 8 November 2019 and takes effect on 26 November 2019.

(2018)[50] which were released for public commentary by the ICT Ministry in August 2018. Between 2018 and 2019, public consultation meetings were held and the Data Protection Policy and Bill, 2018 were forwarded to the cabinet for approval. This was obtained on 18 April 2019. The National Assembly received, deliberated on, and approved the Data Protection Bill, 2019, despite the existence of a similar legislative process before the senate.

Implementation of the DPA, 2019: Extent and challenges

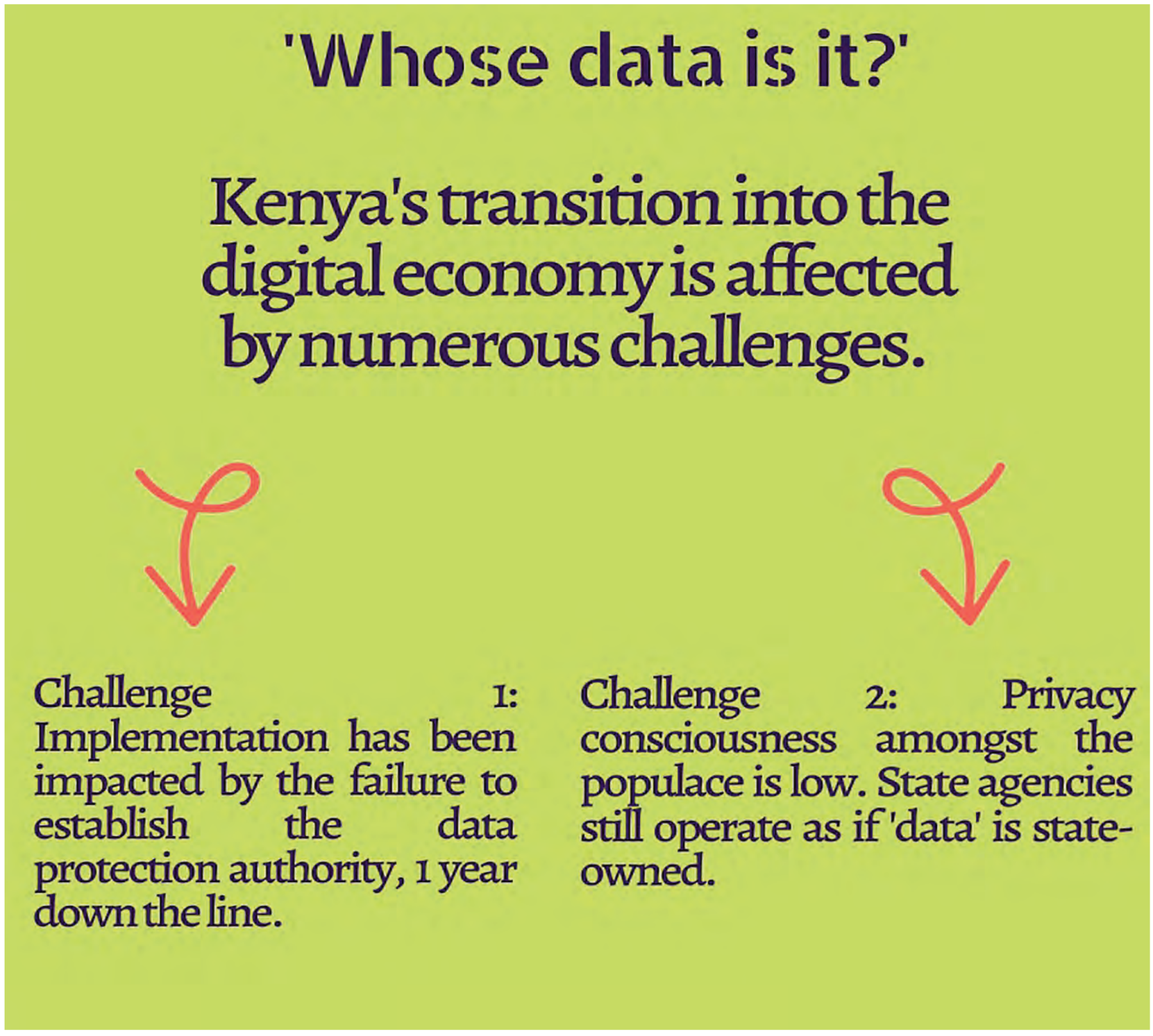
Despite the provisions of the DPA, coming into effect last year, differing opinions persist about the extent and sustainability of its implementation. On one hand, some stakeholders opine that the non-operationalisation of the office of the data protection commission (ODPC) and the attendant "institutional framework" envisaged under the DPA is synonymous with a framework which hasn't been implemented, nearly one month shy of the one-year mark. Drawing on this, some entities noted that they have neither conducted internal data protection impact assessments nor incorporated the DPA's provisions into their policies, structures, processes and general "way of doing things". As one private sector interviewee noted, the "instruments defined in the Act have yet not been put in place."

On the other hand, other stakeholders have been extremely vocal about its ongoing enforceability and implementation and the current enjoyment of rights by data subjects, irrespective of the delayed appointment of the data protection watchdog.[51] This is best evidenced by the petition against

50 Ministry of ICT. (2018). *The Data Protection Bill 2018*. http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf

51 Interview with Gloria Madegwa and Esban Muthoni, case officer and wellness officer at the Defenders Coalition, 12 October 2020.

Edgar Obare, who was charged in August using section 72 of the DPA.[52] As one private sector interviewee noted, they have already "reviewed their internal policies and updated the advice they provide to external parties", despite being bound by confidentiality rules in other legislative and sectoral frameworks.[53]



These divergent opinions on the implementation of the DPA are symptomatic of a deeper attitudinal challenge. While the digital ID conversation heightened county-based awareness about privacy and data protection rights, the COVID-19 pandemic demonstrated

52 The charge sheet read as follows: "On diverse dates between July 9 and July 13, 2020 at an unknown place, within the Republic of Kenya, using your social media accounts , domain name www.bnn.ke and verified Instagram account @edgarobare, unlawfully disclosed to your online followers personal data to wit visa belonging to one Natalie Wanjiru Githinji without her consent." Kimuyu, H. (2020, 3 August). Edgar Obare charged with publication of private data. *Nation.* https://nation.africa/kenya/news/edgar-obare-charged-with-publication-of-private-data-1912154

53 Interview with Mercy Mutemi, legal practitioner at Nzili & Sumbi Advocates, 12 October 2020.

that Kenyans are willing to temporarily shelve their rights[54] and refrain from questioning the wanting safeguards inherent in existing policy frameworks, including the national CCTV Policy.

While no "privacy consciousness" studies have been conducted in the Kenyan jurisdiction, the results of a 2020 Japanese study[55] offer crucial insights into the public awareness and civic education challenges – across different sectors and for different stakeholders – for the ODPC, once operationalised. As two interviewees noted, amongst the HRDs and journalist communities, "low knowledge levels" exist which may impact their work.[56]

These challenges are not merely restricted to the general public, but also private sector and state agency employees. While the former[57] have rolled out internal training and capacity-building initiatives for staff – including GDPR compliance – and are aware of the liability, customer loyalty and business profitability risks,[58] the latter are still driven by the mentality that individuals' personal data "belongs to them." Despite this daunting mentality challenge, the DPA, 2019, if properly implemented, will promote a sustainable paradigm shift,[59] where the balance of power between subjects and controllers/processors is redirected to the individual themselves.

---

54 This is often promoted in the name of grand ideals, namely public interest, public health, and national security, as evidenced by the unchecked roll-out of contact tracing applications by the government and private sector entities.

55 Tabata, N., & Sato, H., & Ninomiya, K. (2020). *Comparison of Privacy Consciousness Between Younger and Older Adults.* Wiley. https://onlinelibrary.wiley.com/doi/full/10.1111/jpr.12284

56 Interview with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

57 This includes ISPs, and entities in the medical, financial and retail sector. Interview with John Walubengo, 10 October 2020. Op. cit.

58 Interview with Ben Roberts, chief technology officer at Liquid Telecom, 9 October 2020. He further stated the need for the ISP sector to "really think about its shared systems and its cloud-based architecture." This was framed around sovereignty issues and the impact of this on client data.

59 Interview with John Walubengo, 10 October 2020. Op. cit.

Building on this, the ongoing compliance at the government level and its current privacy and data protection priorities have been narrowed down to the ongoing digital ID drive,[60] despite the recognition that the government is "not a monolith."

Secondly, there are concerns that the vague and loosely-worded language in the DPA, 2019 not only deviates dramatically from the GDPR (which it is largely modelled on), but also significantly waters down data subjects' rights, controllers/processor responsibilities, and introduces uncertainty into the Office of the Data Protection Commission's (ODPC) mandate. These challenges are core barriers for the proper implementation of the DPA, using the GDPR as a benchmark, and are extensively addressed below.

Data Protection Act: Litigation

The DPA is currently being contested before the High Court of Kenya (Constitutional and Human Rights Division) by Okiya Omtatah. The constitutional petition, which was lodged on 14 November 2019, challenges the constitutional validity of the act as well as the validity of sections 5, 6, 51 (2)(b) and 54, DPA 2019. ARTICLE 19 Eastern Africa successfully intervened as an interested party, and raised additional issues about definitional discrepancies, the failure to balance the right to privacy with freedom of expression and media freedom under section 52, DPA, 2019 and excessively broad exemptions.[61] The petition will be mentioned on 15 December 2020.

60 Ibid.

61 ARTICLE 19. (2019, 25 November). Kenya: Protect the data protection framework. www.article19.org/resources/kenya-protect-the-data-protection-framework

Key data protection issues in Kenya

Key data protection issues persist in Kenya, including issues which were commenced or flagged before the DPA was enacted, but whose determination will shape the trajectory of data protection and privacy in Kenya for years to come. This includes heightened digitisation drives at the state and non-state levels, including drives to roll out a smart city, digital identity drives, the draft CCTV policy,[62] as well as ongoing petitions affecting the right to privacy and data protection.

On the petition front, the High Court in the NIIMS petition issued two crucial orders. The first was the averment that the "collection of biometric (DNA and GPS) data for purposes of identification is intrusive and unnecessary, unconstitutional and a violation of Article 31, Constitution of Kenya, 2010, to the extent that it is not authorised and specifically anchored in empowering legislation."[63] Despite this, biometric (fingerprint) data collection and storage for authentication purposes by private entities, including banks, mobile network operators, health and insurance businesses, continues unabated.

Secondly, the court stalled the continued implementation of Kenya's digital identity system and the utilisation of the NIIMS data, subject to "an appropriate and comprehensive regulatory framework [...] first (being) enacted."[64] On 13 October 2020, the government gazetted the Huduma Namba regulations[65] which

62 Wanyama, J., & Sataar, J. (2019, 7 November). A Commentary on Kenya's Draft National CCTV Policy. *CIPIT*. https://cipit.strathmore.edu/a-commentary-on-kenyas-draft-national-cctv-policy; Amnesty Kenya. (2019, 14 August). Kenya: Desist from Indiscriminate and Invasive Mass Surveillance. https://www.amnestykenya.org/kenya-desist-from-indiscriminate-and-invasive-mass-surveillance/

63 *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020]. Op. cit.

64 Ibid.

65 These include the Registration of Persons (National Integrated Identity Management System) Rules, 2020 and the Data Protection (Civil Registration) Regulations, 2020. Kenya Gazette Supplement No. 176 - Legal Notices No. 195 & 196. https://ict.go.ke; see also Mutua, J. (2020, 16 October). New regulations pave way for Huduma Namba cards. *Business Daily.* https://www.businessdailyafrica.com/bd/economy/new-regulations-pave-way-huduma-namba-cards-2482494

were heavily criticised by stakeholders. [66] Prior to this, the government announced a second round of "mass registration and the mass production of the Huduma Namba cards" following a "data clean up process and the creation of a data centre"[67] in September.

Key features of the comprehensive data protection law

Definitions

Key definitions have been provided under section 2 (interpretation) of the DPA, 2019 but several fundamental weaknesses have been noted. On one hand, it has been noted that the DPA's, 2019 definition of "personal data" is "inconsistent with the definition under the ATI Act, 2016."[68] This comment stems from the fact that the ATI Act, 2016 contains a more detailed definition compared to the constricted definition available under section 2 of the DPA, 2019.

It has also been noted that the definition of the term "sensitive personal data" omits key factors, including "membership of a trade union, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings."[69]

66 ARTICLE 19. (2020, 20 March). Kenya: Digital identity regulations must satisfy constitutional requirements. https://www.article19.org/resources/kenya-digital-identity-regulations-must-satisfy-constitutional-requirements

67 Tanui, C. (2020, 16 September). Huduma Namba e-cards production to begin in December: PS Kibicho. *Capital News*. https://www.capitalfm.co.ke/news/2020/09/huduma-namba-e-cards-production-to-begin-in-december-ps-kibicho

68 ARTICLE 19. (2019, 25 November). Op. cit.

69 Defenders Coalition, Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN), Dr. Robert Muthuri and Privacy International. (2020). *Analysis of Kenya's Data Protection Act, 2019*. https://privacyinternational.org/advocacy/3348/analysis-kenyas-data-protection-act-2019

Data subject rights

The rights of data subjects are mainly provided under section 26, DPA 2019 (rights of a data subject). However, other rights which data subjects possess are scattered in other sections of the framework. These include: the right to data portability and the rights in relation to profiling and automated decision making under section 38 and section 35 of the DPA, 2019 respectively. It has been noted that other rights to guarantee empowerment of data subjects need to be included in the DPA, including an explicit "right to an effective remedy", and a "right to compensation and liability."[70]

Purpose limitations

The principles guiding personal data processing are explicitly set out under section 25 (principles of data protection) which provides that personal data can only be collected for "explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes." This purpose limitation is present throughout the DPA, including section 30 (lawful processing of personal data); section 31 (data protection impact assessment); section 37 (commercial use of data); and section 39 (limitation to retention of personal data), amongst others.

Conditions for lawful processing

The conditions for lawful processing are provided under section 30, DPA, 2019. The conditions required prior to processing include prior consent from the data subject to the "processing for one or

70 Ibid.

more specified purposes." Other scenarios are provided where lawful processing may be permitted.[71]

Relevant exemptions in the public interest

The exemptions applicable under the DPA, 2019 are located under Part VII – Exemptions, and other sections interspersed throughout the framework, including section 30 (1) (b)(iv) and (vi), section 52, amongst other sections.

Specifically, these wide and blanket exemptions are present throughout the whole DPA, 2019, including under section 51 (2) (b), which contentiously exempts the processing of personal data where this is necessary for "national security or public interest". As one interviewee noted, the "government always has a caveat in all laws."[72] Notably, these terms are not defined in the act and risk being abused by state agencies and/or private agencies working conjunctively with the state on public affairs.

This exemption is currently being contested in the data protection constitutional petition, which notes that this provision conflicts with Article 59 (2)(d), Constitution of Kenya, 2010.

Conversely, ARTICLE 19 EA noted that the "journalistic exemption" located under sections 30, 39 and 51, DPA, 2019 inadequately protects the right to free expression. It was noted that this exemption is limited to the processing of personal data and

71 Section 30 (1)(b), DPA, 2019: where the processing is necessary for "for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; for compliance with any legal obligation to which the controller is subject; in order to protect the vital interests of the data subject or another natural person; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; the performance of any task carried out by a public authority; for the exercise, by any person in the public interest, of any other functions of a public nature; for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or for the purpose of historical, statistical, journalistic, literature and art or scientific research."

72 Interview with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

retention provisions, but not to other crucial aspects, including the "requirements of registration of data processing, the processing of sensitive data, the limits on the transfer of personal data outside Kenya and the application of criminal offences."[73] This exposes journalists to serious consequences, including the risk of criminal penalties for articles published in good faith.

Breach notification requirements

The notification and communication of breach requirements are set out under section 43, DPA, 2019. This section inserts a worryingly low notification threshold, when there is "real risk of harm to the data subject." A joint analysis revealed that this threshold is vague and no criteria of risk and likelihood is provided in the section. This vagueness can constitute a loophole for data controllers who hide behind subjective determinations of risk.[74]

Cross-border data transfers

The transfer of personal data outside Kenya is provided under Part VI of the DPA, 2019. Section 48 provides for the "conditions for transfer out of Kenya", Section 49 provides for "safeguards prior to transfer of personal data out of Kenya" and Section 50 provides for the contentious data localisation requirement, or "processing through a data server or data centre in Kenya". Notably, Regulation 38 of the Data Protection (Civil Registration) Regulations, 2020 provides that civil registration entities "shall not transfer personal data collected for civil registration purposes outside of Kenya, except with the written approval of the Data Commissioner."

73 ARTICLE 19. (2019, 25 November). Op. cit.

74 Defenders Coalition, Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN), Dr. Robert Muthuri and Privacy International. (2020). Op. cit.

It is crucial to note that interviewees maintained that the Taskforce Bill (2018) – which relied on the GDPR as the reference document – did not contain the "data localisation" provision under section 50, DPA, 2019. It is unclear whether this was introduced during the cabinet approval stage, and therefore not subjected to public participation, or during the deliberations of the National Assembly, where the committee and the house possess ultimate decision-making powers, irrespective of the public's sentiments.

Other relevant features

Other features have drawn the attention and concern of stakeholders. These include the penalties for breach under section 63, DPA, 2019 (administrative fines), and the use of loose language which will have an impact on data subjects' rights and controllers' or processor responsibilities.

The former provision curiously states that the data commissioner can impose a maximum penalty of "up to five million shillings (approximately USD 50,000), or in the case of an undertaking, up to one per cent of its annual turnover of the preceding financial year, whichever is lower." This poorly-phrased section may permit entities with parent-subsidiary arrangements to negotiate the amount of fines they will pay, which fails to promote their use as a redress mechanism for data subjects.

The use of the word "may" also waters down significant protections in the DPA, 2019. For example, under section 24 (designation of the data protection officer), data controllers and processors have the option to appoint a data protection officer, as opposed to the mandatory appointment envisaged under Article 37 of the GDPR. This is an issue because the DPA, 2019 is supposed to be compliant with international standards.

In preparing this report, responses from interviewees about the financial, regulatory and compliance costs of adhering to rights-frameworks, including the DPA, 2019 were sought. While most interviewees noted that the failure to implement the DPA in a staggered manner[75] for entities with different capabilities may impose a disproportionate burden on all entities, especially micro, small, or medium enterprises, compared to their larger private counterparts, it was also affirmed that one should refrain from "putting a cost on human rights, given Kenya's fledgling entry into the digital economy."[76]

Lastly, it was noted that, in the COVID-19 context, numerous entities have had to shift their way of doing things, including upgrading from paper-based to cloud-based services.[77] This latter point magnified that rights protections and their attendant costs will always be equalised by the free market.[78]

Data protection authority (DPA) or other institutions assigned with the responsibility to oversee rights to personal data protection

Establishment and composition of the DPA and other institutions

The ODPC, which is constituted as a state office rather than a constitutional commission, is established under Part II — Establishment of the Office of Data Protection Commissioner. This office is steered by the data commissioner, and other supporting staff appointed by the data commissioner. The

75 Interview with Grace Mutung'u, 12 October 2020. Op. cit.

76 Ibid.

77 Interview with Ben Roberts, 9 October 2020. Op. cit.

78 Interview with John Walubengo, 10 October 2020. Op. cit.

commissioner is expected to establish relevant directorates, in conjunction with the cabinet secretary (section 5, DPA, 2019).

The recruitment of the data commissioner is initiated by the Public Service Commission, which puts out the call for recruitment and shortlists "three qualified applicants in the order of merit for the position of Data Commissioner" for presidential nomination, subject to the approval of the national assembly (section 6, DPA, 2019). The qualifications required for the data commissioner are elucidated under section 7, DPA, 2019 and unlike other jurisdictions, the commissioner will serve for a "single term of six years" without the possibility of reappointment.

On 14 April 2020, the Public Service Commission issued a public notice for the position[79] and subsequently shortlisted 10 candidates for the position in July 2020. This process was halted by the Employment and Labour Relations Court in July following a petition lodged by Adrian Kamotho. The petitioner contested, among other issues, the time taken by commission (two months) to conclude the recruitment process, in contravention of the 21-day statutory period provided under section 6 (3), DPA, 2019. Reports indicate that petitioner and the commission filed a consent before the court, and the commission "agreed to start the process afresh 'in accordance with the law.'"[80] This fresh recruitment process resulted in 12 candidates being shortlisted.[81]

On 13 October 2020, reports emerged that Immaculate Kassait had been nominated by the President of Kenya for the position of data commissioner, pending the approval of the national

79 https://www.careerpointkenya.co.ke/2020/03/data-commissioner-psc

80 Kiplagat, S**.** (2020, 28 July). PSC back to drawing board on Data Commissioner recruitment. *Business Daily*. https://www.businessdailyafrica.com/bd/economy/psc-back-to-drawing-board-on-data-commissioner-recruitment-2297110

81 Otieno, B. (2020, 15 September). SC shortlists 12 candidates for data commissioner post. *Business Daily*. https://www.businessdailyafrica.com/bd/news/psc-shortlists-12-candidates-for-data-commissioner-post-2301252

assembly's Departmental Committee on Communication, Information and Innovation.[82] It is unclear who the other two shortlisted candidates were. Finally, it is unclear how the High Court will determine the grounds raised in the data protection petition, which raises issues about the recruitment process.

Mandate of the DPA/other institutions

Under section 8, DPA, 2019 (functions of the Office), the ODPC is tasked with "increasing legal certainty"[83] by overseeing the general implementation of the DPA, exercising oversight over data controllers and processes via registration, investigating complaints of privacy and data protection infringements, public education and awareness, promoting international cooperation in matters, and undertaking research on data developments, amongst others. Under section 9, DPA 2019 (powers of the office), the ODPC possesses regulatory, investigative, dispute-resolution, inspection, audit and sanction powers, amongst others.

Effectiveness and challenges of the DPA/other institutions

The ODPC – once operationalised – will face pre-existing challenges which will drastically affect its effectiveness, and limit its ability to work independently.

The first challenge of the ODPC's office is its lack of independence and its situatedness as a state office under the ICT Ministry, which is itself a state agency and a data controller/processor. While some interviewees noted the need to recall practical realities within the Kenyan jurisdiction, including the

82 https://www.youtube.com/watch?v=kFgmxsvG2qs

83 Internet Society & Commission of the African Union. (2018). *Personal Data Protection Guidelines for Africa.* https://www.internet-society.org/resources/doc/2018/personal-data-protection-guidelines-for-africa

Kenya's Data Commissioner

General function under section 8, DPA, 2019:

- Oversee the implementation of and be responsible for the enforcement of this Act.

General powers under section 9, DPA, 2019:

- Regulatory, investigative, dispute-resolution, inspection and audit, and sanctions powers.

Challenges and Risks:

- The Commissioner faces pre-existing restrictions, including power-sharing with the Cabinet Secretary, ICT Ministry. This will drastically affect its effectiveness and limit its ability to work independently.
- This risks affecting Kenya's nascent privacy and data protection practice, and consequently, the rights of Kenya's 47.6 million data subjects.

fears of a constitutional commission being subjected to arbitrary budgetary cuts in a similar manner to constitutional commissions (i.e. KNCHR and CAJ) and parastatals which may interfere with the governments operations, it is concerning that these realities took precedence over the full protection and promotion of the right to privacy and data protection in Kenya.

Secondly, as noted above, the ODPC faces the challenge of combating attitudinal problems within the government itself, which still possess copious privileges in the data collection, processing and storage arena.[84]

Thirdly, interviewees queried the ability of the ODPC to effectively deal with an anticipated case-load challenge in a timely manner, including complaints, which will likely be placed before it.[85]

84 Interviews with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

85 Ibid. This query, prior to the establishment of the ODPC, led to a pertinent statement about the "type of measures which can be created before the Commissioner takes office."

Fourthly, Section 8 (1)(d), DPA 2019 promotes self-regulation among data controllers and data processors. This provision risks eroding the protections contained in the DPA, given the failure to specify instances where self-regulation is permitted, for what types of controllers and processors, and the safeguards which will be implemented to prevent abuses. It is also unclear how this self-regulation will be aligned with the codes and guidelines which the ODPC must issue under section 74, DPA, 2019.

Lastly, it is unclear why the cabinet secretary, ICT Ministry possesses wide powers under the DPA and the justification for this. However, it is certain that this risks disempowering the ODPC and may permit the ICT Ministry to interfere in the functions of the ODPC, without the need for prior consultation.

This is evidenced by the following provisions; section 35, DPA, 2019 (automated individual decision making) empowers the cabinet secretary, rather than the ODPC, to "make such further provision to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of decisions based solely on automated processing." Section 37, DPA, 2019 (commercial use of data) empowers the cabinet secretary, in consultation with the commissioner, to "prescribe practice guidelines for commercial use of personal data in accordance with this Act." Section 50, DPA, 2019 (processing through a data server or data centre in Kenya) grants the cabinet secretary *exclusive* powers to "prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya."

Data protection practices in internet country code top level domain name (ccTLD) registration

Kenya's .ke ccTLD (domain) registration services are "administered by KENIC" and the communications authority of Kenya acts as the "trustee [...] on behalf of the Government of Kenya".[86]

KENIC has an interactive WHOIS search query webpage permitting access to domain, contact, host and registrar information.[87] Further, KENIC's .ke Domain Name WHOIS Policy stipulates that the registry is permitted to publish certain personal data, including: "name, address and telephone and fax number of the Registrant; technical contact person; email address of Registrant; technical data (such as status of the Domain Name or the name servers)."[88] The policy further asserts that the contact information for private individuals is "restricted to the email address, unless they request otherwise."[89] Individual registrants are explicitly informed about the ability to "create and use a specific functional email address for publication in the WHOIS as an alternative to the use of their personal email address."[90]

The policy also specifies that it will only transfer personal data to third parties where it is "ordered to do so by a public authority, carrying out its legitimate tasks."[91] Third parties are required to fill in an application form and provide supporting information, as well as agree to certain disclaimers.

86 https://ca.go.ke/industry/e-commerce-development/domain-name-system

87 https://whois.kenic.or.ke/whois.jsp

88 https://kenic.or.ke/policies

89 Ibid.

90 Ibid.

91 Ibid.

Lastly, KENIC provides third parties with access to personal data, where it has been ordered to do so by a "judicial authority in Kenya". It is unclear whether KENIC has dealt with such requests, including from law-enforcement agencies, whether court-sanctioned warrants were produced beforehand, and whether it publicly discloses this practice on its website. An email request for information was submitted to KENIC on 9 October 2020, but no response had been received as at 19 October 2020.

Analysis in line with AfDec and other relevant instruments

Kenya's DPA, 2019 is a representation of the tireless efforts by numerous internal and external stakeholders. Despite this, the legislative framework lacks full informational privacy protections, as evidenced by the extensive loopholes documented above. This is also informed by the fact that the DPA does not conform with international and regional best practices and standards, including those on protection and privacy.[92]

Notably, Principle 8 of the AfDec mandates that the right to personal data protection must be provided for *all* stakeholders. Despite this, Kenya's DPA, 2019 falls below this standard by failing to provide adequate protections for children. Secondly, the right to communicate anonymously on the internet and using digital technologies is not fully guaranteed, given the existence of competing legislation which waters down this right. Thirdly, the DPA, 2019 fails to meet the three-part test and includes broad, vague and ill-defined restrictions on personal data protections which are inconsistent with these permissible restrictions.

92 Interview with Gloria Madegwa and Esban Muthoni, 12 October 2020. Op. cit.

Fourthly, the DPA, 2019 fails to comply with other regional guidance, including the AU Convention, the Personal Data Protection Guidelines for Africa and the ACHPR Declaration. Despite Kenya not being bound by these three documents, all of them emphasise the need for an independent data protection authority as a "vital element of the legal and institutional framework for building trust online."[93] As noted above, Kenya falls far below this standard.

Crucially, Kenya supported recommendations to "revise and enact the draft data protection bill and create a data protection framework in line with international standards on the right to privacy,"[94] despite the enactment of the DPA, 2019. This is a crucial recognition by the state that its current framework is not on a par with these regional and international commitments, which was echoed in CSO reports.

Lastly, despite Kenya's DPA being modelled on the GDPR, Kenya has not taken further measures to address the inconsistencies noted above by aligning and updating the framework.

Analysis of the status of a human rights-based approach to personal data protection in the country

The draft "Privacy and Personal Data Protection in Africa – Advocacy Toolkit" magnifies the utility of the human rights-based approach, and notes that this helps "policy makers perform better at meeting their human rights obligations, and have better outcomes that benefit rights-holders."[95] This

93 Internet Society & Commission of the African Union. (2018). Op.cit.

94 "142.28 Revise and enact the draft data protection bill and create a data protection framework in line with international standards on the right to privacy (Estonia); 142.176 Ensure that surveillance and profiling of citizens respect the right to privacy, including judicial oversight (Germany)". UNHRC. (2020). *National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21 - Kenya*. https://undocs.org/A/HRC/WG.6/35/KEN/1

95 https://africaninternetrights.org

approach is underpinned by the "PANEL" principles (participation, accountability, non-discrimination and equality, empowerment, legality),[96] which will be explored below.

Despite Kenya's 12-year-old informational privacy journey, the five principles were not uniformly applied during the various open and closed deliberation processes.

Participation and non-discrimination and equality

On the participation front, the formation of the task force commendably opened up processes permitting more individuals and organisations to actively take part in the public participation processes. However, the selection criteria used to identify the members of this task force remains unknown. Secondly, the continued failure to enact the draft Public Participation Bill (2019)[97] means that public consultation hearings giving effect to public participation provisions in the Constitution of Kenya, 2010, left out various stakeholders. This included persons with disabilities, children and the elderly, amongst others, whose voices were glaringly absent from the data protection process between 2007 and 2019.

Commendably, the National Assembly process prioritised public *county* meetings, which encouraged a shift towards a more holistic, nation-based rather than Nairobi-based, approach to data protection and privacy in Kenya. This helped shatter the existence of geographical barriers, and the exclusion of individuals on this basis, in ICT policy processes in Kenya.

96 http://ennhri.org/about-nhris/human-rights-based-approach

97 http://kenyalaw.org/kl/index.php?id=9091

Accountability

Under the “accountability” umbrella, the lack of appropriate mechanisms capable of holding duty bearers to account for this failure to include all voices as mandated under the Constitution of Kenya, 2010, resulted in individuals turning to the courts. Kenya’s judicial process is not only expensive, and time-consuming, but also adversarial. These factors reveal the need to enact out-of-court redress and accountability mechanisms, during bill formation processes, given the inadequacy of existing mechanisms.

Secondly, as magnified above, Kenya does not mandate data controllers and processors to appoint data protection officers capable of promoting institutional compliance, at the state and private entity levels.

Empowerment

Empowerment is synonymous with an individual’s ability to *know* and to *choose*. As noted above, one of the core implementation challenges awaiting the ODPC is the pressing lack of “privacy consciousness”. This will require the office to actively and deliberately tailor specific education and awareness-raising campaigns, across the country, which must be available in both official languages in Kenya, Kiswahili and English. This, as noted in the draft toolkit, will provide a threshold against which to measure the “effectiveness (i.e. use) of the law”.

Secondly, easily accessible platforms must be available to individuals permitting them to exercise their data rights, which requires on-the-ground harmonisation and interoperability of systems and processes.

Legality

The challenges of the legality of the DPA, 2019 have been enumerated extensively above. These legality challenges, which are being contested before the High Court, will have an impact on the viability and effectiveness of the DPA, including for future generations.

Concluding observations and recommendations

The documented information reveals that Kenya's DPA, 2019, whilst a step in the right direction for informational privacy, leaves a lot to be desired. Despite the Kenyan government affirming the existence of gaps in the draft Data Protection Bill, during its UPR review, it still failed to enact a framework "in line with international standards on the right to privacy".[98] Kenya's framework does not offer data subjects the panacea and liberation proponents sought, given the existence of internal and external inconsistencies, including on issues which are central to its practical and sustainable implementation and competing legislation.

As noted above, the various open and closed processes – from 2007 to 2019 – which led to the enactment of the DPA, 2019 were marked with notable successes and failures which impacted Kenya's "PANEL" assessment. On one hand, positive efforts were made to shatter the Nairobi-centric nature of the data protection conversations during the 2019 National Assembly deliberations, and to solicit the input of vast stakeholders during the 2018 taskforce deliberations. However, the inability to promote participation by *all* rather than *aware* stakeholders affects the conclusion that Kenya's DPA, 2019 offers data protection "for *all* stakeholders" (Principle 8 of the AfDec). Further, the existence of

98 UNHCR. (2020). Op. cit.

a constitutional petition casts a still undetermined shadow on the constitutionality of the DPA, 2019.

Lastly, Kenya's ODPC faces the challenge of rousing "privacy consciousness" amongst rights holders and duty bearers in the Kenyan jurisdiction. Where this is collaboratively pursued, an accountable, participatory and trust-laden transition into the digital economy may be possible.

Recommendations: Strengthening the privacy and data protection framework and application of the human rights-based approach.

To the government:

- Commence a stock-taking review of the DPA, 2019 to assess what progress and challenges exist in the Kenyan jurisdiction, nearly a month to the one-year mark.
- Urgently commence sensitisation and public-awareness training and capacity-building sessions to combat state agencies' perceptions (individual and organisation level) about the ownership status of personal data.
- Actively promote the inclusion of excluded stakeholders to ensure a deeper, and wider level of participation.

To civil society organisations and academia:

- Continue advocating for the sealing of loopholes and inconsistent provisions in the DPA, 2019, including before national, regional and international judicial fora.
- Continue monitoring ongoing behaviour by data controllers and processors in Kenya and utilise right-to-information requests to solicit information from state and non-state actors.

- Continue documenting data protection and privacy successes and challenges in shadow reports, including before the UNHRC (ICCPR state review), the OHCHR (UPR) and the ACHPR (observer status reporting mechanism), amongst others.

To the private sector (ISPs and MNOs):

- Internalise DPA, 2019 responsibilities and take initiatives to ensure compliance, irrespective of the non-operationalisation of the ODPC.
- Commence user and client sensitisation about updated privacy policies.
- Promptly inform users and clients – using online and offline platforms – about the occurrence of data breaches.

To the technical community:

- Publicly disclose the number of WHOIS law enforcement requests and their resolution.
- Implement the data protection by design and default provisions into internet and technology infrastructural systems and processes.