Is that even legal?

A guide for builders experimenting with data governance in Kenya

February 2023
By Lawyers Hub
About Mozilla

Mozilla’s mission is to ensure the internet is a global public resource, open and accessible to all. An internet that truly puts people first, where individuals can shape their own experiences and are powerful, safe, and independent.

Founded as a community open source project in 1998, Mozilla currently consists of two organizations: the nonprofit Mozilla Foundation, which leads our movement building work; and its wholly owned subsidiary, the Mozilla Corporation, which leads our market-based work, including the development of the Firefox web browser. The two organizations work in close concert with each other and a global community of tens of thousands of volunteers under a single banner: Mozilla.

Acknowledgements

We would like to thank Stefan Baack, Solana Larsen, and Kasia Odrozek, who provided valuable feedback on this work. We also thank Kristina Shu and Nancy Tran from Mozilla Foundation’s design team for their support in designing this report. Ran Zheng created the illustrations you’ll find throughout these pages. Thanks are further due to J. Bob Alotta, Champika Fernando, Mehan Jayasuriya, EM Lewis-Jong, Jackie Lu, Anouk Ruhaak, Udbhav Tiwari, and Richard Whitt for informing the direction of this project.

This work was led by Mozilla’s Insights team. Eeva Moore led design and engagement work, Kenrya Rankin edited the research, and Neha Ravella provided project management support. Maximilian Gahntz was the project lead.

Disclaimer

The views expressed in this report represent those of the authors. The report’s content does not constitute legal advice. Please seek the advice of a qualified attorney.

This work is licensed under the Creative Commons Attribution 4.0 (BY) license, which means that the text may be remixed, transformed and built upon, and be copied and redistributed in any medium or format even commercially, provided credit is given to the author. For details go to http://creativecommons.org/licenses/by/4.0/.
# Table of Contents

**Preface**
- Overview ........................................................................... 3
- How to read this guide .................................................. 4

**Background** .................................................................. 5

**Overview of the legal landscape** ........................................ 7
- Constitution of Kenya, 2010 .................................................. 9
- Data Protection Act, No. 24, 2019 ......................................... 11
- Data protection regulations ................................................ 13
- Basic Education Act, No. 14, 2013 ........................................ 14
- Kenya Information and Communication Act, 1998 ................. 14
- The Computer Misuse and Cyber Crimes Act, No. 5, 2018 .... 14
- Consumer Protection Act, 2012 .......................................... 15
- The National Payment System (NPS) Act, 2011, and NPS Regulations, 2014 .... 16

**Case Study: Alternative Data Governance Approaches in Kenya** ............... 17
- Data sharing pools ............................................................ 17
- Data commons ................................................................. 21

**Bibliography** ................................................................ 25
Preface

By Mozilla Insights

It’s a long-established fact: today’s data economy is not built on a level playing field. The people and communities whose data form its lifeblood are fighting to retain or regain control over their data and the value created from it. All too often, data is extracted and processed far removed from its source, serving the interests of the organizations that collect it rather than the people it impacts. This is why it’s important to explore new ways to govern data: to shift control, strengthen agency, to share value. Through the Mozilla Foundation’s Data Futures Lab and our work around data governance, we are working to challenge this current paradigm.

Reimagining, reconstituting, and rebalancing data governance requires system-level change, but opportunities to implement new ideas for better data governance often also exist within existing paradigms and legal frameworks. Just as the open source movement challenged copyright laws to introduce open licensing decades ago, builders can similarly defy existing laws and regulations to push the boundaries of how data is governed. Builders can shape new norms by leveraging opportunities present in existing rules. But to do so, they need a firm understanding of current realities. We aim to help them navigate existing legal landscapes so they can help pave the way for better data governance models and policy in the future.

The primary goal of this research is therefore twofold:

- To provide builders with an overview of the current (and changing) legal landscape governing the collection, management, sharing, and use of data in their country;
- to identify opportunities for what we call “alternative data governance” models within existing legal landscapes — specifically, where the regulatory status quo offers pathways to implement new approaches that shift power from data
collectors to data subjects — that create meaningful incentives for the benefits of data to be shared between various parties and enable data to serve individual or collective interests.

The guiding question is: What can be built where, and using which levers, from a regulatory standpoint?

The analysis in this guide will provide builders with a map of laws and regulations relating to data and opportunities for experimentation, along with key questions for builders to ask.

Overview

The report begins with a section providing general background on the topic of data governance. From this starting point, it explores the landscape of Kenya’s nascent legal data governance framework and adjacent areas of the law. Most notably, it discusses the rights to privacy and access to information under Kenya’s 2010 Constitution and key laws and regulations like the 2019 Data Protection Act and subsequent Data Protection Regulations.

The report then explores potentially promising alternative approaches to data governance in Kenya and lists key questions for builders to consider. The first is the data sharing pools (or data collaboratives) model. These platforms facilitate the pooling and sharing of data between organizations to help derive collective insights and shared value. The idea is to treat data as a shared resource instead of a rivalrous one.

The second approach the report explores is data commons, a shared resource stewarded by a community with the goal of making it more widely accessible and useful. The data held as a commons is governed by shared rules and norms developed by the community.
How to read this guide

This report is a reference that does not need to be read from cover to cover in a linear way; you can simply dip in and out of different sections as needed. You will further find brief summary boxes with key themes and findings from each section.

What this guide does not include is legal advice. It rather aims to provide a starting point in your exploration of this topic to help you ask the right questions and identify areas where bespoke advice from lawyers is necessary.

Background

The importance of data as the key input of the data economy — and a key factor for people’s wellbeing in the data economy — calls for effective data governance. This needs to consider individuals' rights and requires effective models of managing and using data. It also needs to ensure compliance with existing regulatory frameworks. Data governance is a combination of different functions and activities encompassing the creation/collection, maintenance, use, and disposal of data. As such, effective data governance requires the identification, organization, and classification of (personal) data; an understanding of data flows within and beyond an organization; documentation; and clear accountability mechanisms. In particular, effective data governance ensures data quality and security to protect the interests of data subjects.

To address the imbalances between data collectors and subjects and move away from the hegemonic data governance model that is pervasive in the data economy — where data collectors control data collection, access, use, and processing — there is a need to consider alternative approaches to data governance. Some of these challenges are particularly pronounced in the Global South, where several countries lack data protection laws.
As defined by Mozilla, alternative data governance refers to "rules and processes that shift power from data collectors to data subjects; create meaningful incentives for the benefits of data to be shared between various parties; and that enable data to serve individual or collective interests grounded in human rights, data rights, and consumer rights."\(^1\) In short, the goal is to strengthen people’s agency over their data and allow them to share in the value created from it. Alternative approaches to data governance can also provide alternatives to market-driven models that center the interests of data subjects, communities, and the general public. Examples of such approaches include data cooperatives, data commons, data collaborative (sharing pools), and data fiduciaries.\(^2\)

The implementation of alternative data governance approaches has been hampered by issues that include a lack of data infrastructure, limited access to data, a wide skills gap, and unconducive regulatory frameworks. Further, concepts like data stewardship, data commons, and data cooperatives have had little traction within Kenya so far.\(^3\) The objective of this report is to grow awareness of this issue area, help Kenyan builders comply with the existing regulatory framework for data governance, and experiment with data governance in ways that advance the interests of data subjects.

---


Overview of the legal landscape

In this section:

- Kenya’s legal data governance regime is still nascent. The 2010 Constitution of Kenya first enshrined the rights to privacy and information and laid the basis for new legislation.

- Most notably, the Data Protection Act of 2019 and the subsequent Data Protection Regulations regulate the collection and processing of personal data in Kenya and prescribe key data protection principles and obligations for builders.

- In addition, a number of other laws, like the Kenya Information and Communication Act and the Consumer Protection Act also touch on how people’s data must be handled.

Kenya’s legal data governance regime is still in its formative stages, which requires builders to keep up with new and ongoing developments in policy and the law. At the same time, the legal landscape also continues to evolve, shaped by lawsuits like the Huduma Namba Case⁴ (which challenged the roll out of Huduma Cards for being outside the scope of the Data Protection Act)⁵ and initiatives like the Kenya Open Data Initiative (a public portal used by the government to release large datasets to the public). The result: the government is being challenged to advance and set an example with regard to data protection practices and openly accessible data.

Both data protection and the increased level of open government initiatives are therefore trends that builders should pay close attention to. The inauguration of the Constitution of Kenya in 2010 guaranteed citizens’ right to government information⁶ and right to privacy.⁷ Kenya subsequently enacted the Data Protection Act in 2019 to give effect to the constitutional right to privacy and the regulation of personal data processing. For open government to be effective, it must be tied to data protection —

---

⁴ Republic v. Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 Others; ex parte Katiba Institute & Yash Pal Ghai (2020).
particularly because of the large sets of data involved, the types of data being processed (which could include personal data), the different parties that may have access to the data, the systems used to hold/store these datasets, and the duration of initiatives.

In tapping into initiatives that support open data, builders can reap the benefits of interacting with publicly available data to develop solutions to benefit the public. But they also need to shoulder the responsibility to ensure that data is well managed and protected. This makes it crucial to implement the rights to information and privacy in a way that ensures both the promotion of access to information and protection and good management of the data in question.

Legislative and policy interventions so far take into account various ways that data can be managed, such as through data protection laws, consumer protection laws, financial laws, and cybersecurity laws. These laws are relevant to builders because they impact industry practices through various compliance and regulatory requirements. This legal framework identifies to what extent you can collect, manage, and share information. For instance, under the Basic Education Act in Kenya (see more below), the County Education Board must establish a database of data about institutions of learning, training, and research. Furthermore, the personal data of the teachers and students is also collected and stored.  

Currently, data governance in Kenya is controlled by a number of laws and regulations. Builders should be familiar with this legal framework, as it stipulates your duties and responsibilities as data collectors and processors. Failure to comply could result in infringement of data rights, leading to costly litigation and administrative sanctions. These laws and regulations include the constitutional foundation, data protection law, and municipal rules.

---

Section 79, Basic Education Act No. 14 of 2013.
Constitution of Kenya, 2010

The Constitution of Kenya of 2010⁹ (CoK) provides the foundational rules and principles for data governance in Kenya — first, through the right to privacy and, secondly, through the right to access information.

The right to privacy

Articles 31(c) and (d) of the CoK guarantee the right to privacy for all persons concerning family/private affairs and communications. That means the CoK champions the personal data sovereignty model, where data subjects have significant control over processing their personal data and there is a drive for processing data based on the data subject's consent. As a builder, this requires you to process and manage data with due consideration of the right to privacy. Importantly, the right to privacy is enforceable by any person claiming denial, violation, infringement, or threat. Thus, builders must ensure that data protection concerns are incorporated into organizational policies and procedures, including product development.

The right to access information

The Constitution also guarantees persons the right to access information.¹⁰ This right empowers people to access information and data that is held in both the private — as it relates to the exercise of their rights — and public sector, and mandates public institutions to publish and publicize information that impacts the general population. It further gives every person the right to correct or delete any "untrue or misleading information that affects the person."¹¹ The right to access information is an enabling right for the enforcement of other socioeconomic rights that builders need to consider when making data available, including the use of personal data in the private or public sector.

---

The Kenya Open Data Initiative is an example of a program that promotes access to information for the citizenry. In a bid to enhance transparency, it provides information that is publicly accessible for the common good and illustrates government efforts to enable access to public government data.\textsuperscript{12} The first data published on the portal was data from the census in 2009, expenditures at the national and regional level, and information on public services.\textsuperscript{13} At the regional level, the Africa Open Data Network increases the use of open data\textsuperscript{14} by serving as a community of Africans, and friends of Africa, who believe that open data can help advance the continent’s development agenda.

It is important for builders to exercise the right to access information in a way that does not constrain the right to privacy. Access to information related to personal data is subject to limitations and safeguards that include the unwarranted invasion of an individual’s privacy (other than the applicant or the person on whose behalf an application to access information has, with proper authority, been made).\textsuperscript{15} Thus, builders must always consider the secondary effects of access to information.

Courts have also addressed issues pertaining to information access and directed, for example, that details of contracts signed to implement public projects be publicly available. For instance, the Standard Gauge Railway project raised concerns about transparency, leading to a public interest suit where the court directed that the contract details be made available to the public.\textsuperscript{16} Similarly, the government — through the


\textsuperscript{13} Raed M. Sharif, “Utilization and Value of Public Sector,” (Dissertation), Syracuse University, 2013, https://surface.syr.edu/cgi/viewcontent.cgi?article=1085&context=it_etd.


\textsuperscript{16} Kenya Law, “Constitutional Petition 159 of 2018 & 201 of 2019 (Consolidated),” accessed October 31,
Kenya Data Portal — has released financial data so citizens can examine how the government manages public resources, such as expenditures on national health.

The rights to privacy and access to information are complementary and seek to ensure accountability and the protection of data subjects from state overreach. The benefit is that the public is actively participating in government. Therefore, privacy should not be construed to mean that government systems and processes should not be transparent or accountable. Transparency in the use of data should be interpreted as the need for citizens to understand how government decisions are made based on their data.

Data Protection Act, No. 24, 2019

The Kenyan Data Protection Act (DPA) was enacted in 2019, giving effect to the right to privacy. The DPA regulates the collection and processing of personal data. It also established the Office of the Data Protection Commissioner to enforce the DPA.

Section 25 of the DPA enlists principles of data protection, which require builders to:

- conduct all processing activities in a manner that is in accordance with the right to privacy of the data subject, in a manner that is lawful, fair, and transparent
- ensure that collection of data is for explicit, specified, and legitimate purposes
- ensure the data is accurate and kept up to date
- ensure that personal data transferred outside Kenya is subject to adequate data protection safeguards or data subjects’ consent
- follow the principle of necessity, which requires you to collect the minimum necessary data for a specified purpose

---

Section 26 requires processing that is compliant with the rights of the data subjects. Builders need to be mindful of the rights that include:

- the right to be informed of the use of personal data
- the right to access the data
- the right to object to the processing of all or part of personal data
- the right to correction and/or deletion/erasure of false or misleading data
- the collection of data in a transparent manner and for a legitimate purpose

According to Section 31 of the DPA, processing of sensitive personal data (i.e., data revealing race, health status, ethnicity, social origin, conscience, belief, genetic and biometric data, property details, sex, sexual orientation, marital status, or family details such as children, parents, and spouses) must be preceded by a Data Protection Impact Assessment (DPIA). A Data Protection Impact Assessment ensures that the builder is able to describe the envisaged processing operations and the purposes for such processing, assesses the necessity and proportionality of the processing operations as they relate to the purposes described, evaluates the potential risk to the rights and freedoms of the data subjects, and appraises the consequent safeguards and security measures put in place as a result. The DPA also provides for notification of breaches that have harmed or risk harm to the rights of the data subjects; data processors and controllers have the obligation to report and notify the data subject (without delay) and the data protection commissioner (without delay, within 72 hours).

In developing solutions for people younger than 18 years old, you must take extra steps, such as enabling guardian monitoring and preventing breaches relating to data relating to children. Additionally, builders must ensure that technology and programs do not lead to exclusion or discrimination. Algorithms deployed in the analysis of characteristics of data subjects, based on their data, should allow a natural person to confirm the decision made by the algorithm.

---

Data protection regulations

Three data protection regulations were developed to aid implementation of the DPA:

- **The Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021:**
  governs compliance and enforcement mechanisms for the regulator, data controllers, and data processors

- **The Data Protection (General) Regulations, 2021:**
  governs procedures for enforcing data subject rights and outlines the duties and obligations of data controllers and data processors

- **The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021:**
  governs registration requirements for data processors and controllers — including companies engaged in product development where personal data is involved — and requires them to register with the Office of the Data Protection Commissioner; requires builders to comply with the abovementioned principles of data protection

Builders are required to establish practices that mitigate risks to personal data; facilitate access to personal data; and have it rectified, restricted, or deleted. Moreover, builders must establish technical and organizational measures that enable the data subject to exercise their rights. This, in turn, promotes the interests and rights of end users who have a right to know how their personal data is processed. Furthermore, the right to be informed of data processing activities puts data subjects at the center of organizational decision-making, thus promoting transparency.

---


Basic Education Act, No. 14, 2013

The Basic Education Act ensures that Kenyan children have access to free and compulsory primary education.\(^{25}\) Section 79 of the Basic Education Act prescribes that the County Education Boards established under the act maintain a database of all registered, accredited, licensed, and incorporated institutions of education, training, and research — and the teachers and students within their walls. Although the database is open to the public, builders in the education sector need to consider measures to protect the information from unauthorized access, use, and manipulation.

Kenya Information and Communication Act, 1998

The Kenya Information and Communication Act (KICA) regulates the use of data subjects’ personal information and includes stringent measures for the operation of information and communications technologies systems and products touching on the privacy of persons.\(^{26}\) KICA obliges builders to establish mechanisms to prevent unlawful access to — and unauthorized processing of — personal data. They need to ensure that steps are taken and adhered to so as to secure the integrity of the personal data under the possession or control of a license holder. That means you need to put in place organizational measures to prevent loss of, damage to, and unauthorized destruction of data.

The Computer Misuse and Cyber Crimes Act, No. 5, 2018

The Computer Misuse and Cyber Crimes Act seeks to equip and enable relevant authorities to detect, prohibit, prevent, respond to, investigate, and prosecute computer and cybercrimes.\(^{27}\) To protect data subjects, it provides for offenses relating to computer systems, such as unauthorized access or interference, and unauthorized


interception of communications. The court may also order you to cooperate with government authorities with regard to such interceptions and recordings.\textsuperscript{28}

By virtue of such possibilities, particularly for builders in the telecommunications industry, there is a need to incorporate structures that, in their design and build, factor in the data’s integrity and safeguards for the data. Builders developing data-driven products should consider the availability of cybersecurity specifications, such as disclaimers, policies, and mitigation mechanisms (including threat detection and prevention in software products).

**Consumer Protection Act, 2012**

Kenya’s Consumer Protection Act (CPA)\textsuperscript{29} safeguards the rights and interests of consumers in the market. Regarding data governance, Section 86 of the CPA requires confidentiality to be adopted for information in the market (an express requirement to keep confidential all information relating to data subjects), such as purchasing patterns and decisions. This includes individual data subjects conducting day-to-day business and end users of products and services provided by developers, programmers, and other categories of builders.

Builders working in this context must protect consumers’ security, safety, and fundamental rights, which include the right to privacy. Therefore, consumer protection is a concern for builders of data-driven products and services, as the law requires consumers’ commercial and social interests to be considered.

**Health Act, 2017, and the HIV and AIDS Prevention and Control Act, 2006**

Health data is very sensitive data. Disclosure of health-related information is not permitted unless with consent, a court order, or as permitted by law. Considering its sensitive nature, data processing in the health sector must be handled with particular care. Access is limited only to health care providers. So it’s necessary to guarantee that the technology used in the preservation of medical data considers confidentiality requirements. Developers and service providers operating in the medical field should

\textsuperscript{28} Section 52 and 53, “Computer Misuse and Cybercrimes Act No. 5 of 2018.”

also take into account the risk of data breaches and the legal implications involved, including lawsuits relating to violating the right to privacy.

The National Payment System (NPS) Act, 2011, and NPS Regulations, 2014

The National Payment System (NPS) Act, 2011, and NPS Regulations, 2014, created payment systems and products standards to regulate the processing of personal data in the financial sector. Section 42 of the NPS Regulation requires personal data collected from customers to be kept confidential. Consequently, builders are required to provide solutions for payment system providers, e.g., card payment technologies, to consider the impact of unauthorized data access within the country’s payment systems.
Case Study:
Alternative Data Governance Approaches in Kenya

In this section:

- Alternative approaches to data governance have not gained significant traction yet, but some approaches, like data sharing pools and data commons, have shown promise.

- Data sharing pools are platforms that facilitate the pooling and sharing of data between organizations in order to help derive collective insights and shared value. The idea is to treat data as a shared resource instead of a rivalrous resource.

- Data commons are a shared resource stewarded by a community with the goal of making it more widely accessible and useful. The data held as a commons is governed by shared rules and norms developed by the community.

While alternative data governance models have not (yet) gained traction in Kenya, the current legal framework leaves room for experimentation to push toward a more empowering paradigm of data governance that recognizes individuals and communities as more than recipients of information or providers of consent about how their data is used, and implores them to participate in the process of data collection, use, and sharing.\(^{30}\) This section provides an overview of approaches that have emerged in the Kenyan context, plus examples of initiatives demonstrating their implementation across different markets and sectors.

Data sharing pools

Data sharing pools (or data collaboratives) are platforms through which organizations pool and use similar data in a centralized way. Data sharing pools facilitate the joint collection and maintenance of data, and participant organizations make decisions on which data to share. Therefore, the underlying objective of creating data sharing pools

is to facilitate increased movement of data, reduce the cost of data collection, and ultimately derive collective insights and more shared value from the data.\textsuperscript{31} Data sharing pools can also promote co-ownership, as the data is treated as a shared resource instead of an exclusive commodity, ideally resulting in more data-driven innovation, new products and services, and economic benefits for participants.\textsuperscript{32} In the private sector, for example, data sharing can be useful for combating money laundering and terrorist financing by providing a way to monitor any actor’s aggregated activities across platforms and borders.\textsuperscript{33} Some challenges of data sharing pools can be a lack of standardization, poor data quality, and a lack of (or limited) regulatory clarity around the use of privacy enhancing technologies. It can also be difficult to determine what information may be shared, and with whom it may be shared. Thus it is critical to ensure that data sharing pools are only set up if the parameters are in line with data protection law.\textsuperscript{34} Similarly, data sharing pools must always protect personal and sensitive personal data.

In Kenya, Section 55 of the Data Protection Act\textsuperscript{35} provides for a prospective data sharing code issued by the data commissioner. The code should contain practical guiding steps for sharing personal data that is compliant with the provisions of the


\textsuperscript{32} Marina Micheli, Marisa Ponti, Max Craglia and Anna Berti Suman, “Emerging Models of Data Governance in the Age of Datafication,” \textit{Big Data & Society}, 7(2), (September 1, 2020), \url{https://journals.sagepub.com/doi/full/10.1177/2053951720948087}.


\textsuperscript{34} “High Level Roundtable for Data Pooling, Analysis and Data Protection, 10-11 March 2021.”

Similarly, the Data Protection (General) Regulations, 2021, under Regulation 21, allows organizations to share the personal data they collect upon request by another data controller, data processor, third party, or data subject — if they respect the data protection principles prescribed in the DPA. Additionally, the regulations require the data controller or data processor to make a determination as to the purpose and means of sharing such personal data between data controllers and data processors.

These legal provisions permit the pooling of data in Kenya and therefore allow builders, within the above mentioned parameters, to freely and legally share data amongst yourselves to achieve shared objectives. The relationship must be guided by a contract that sets out the obligations of each of the parties and the standards within which they will operate in processing data, such as security safeguards and rules for sharing data with other third parties. The provisions within such a contract should include:

- The parties involved in the sharing of the data
- Why the personal data is required
- A clear description of the data, including the types of data that will be shared
- Data access mechanisms that detail how the data will be transferred from the providing entity to the receiving entity and names the parties who will have access to the data
- How long the data will be retained
- The obligations and the rights of the parties to the contract, whether data controllers or data processors
- The safeguards put in place to ensure that the data is secure from unlawful disclosure

In Kenya, the data sharing model is being adopted across the transport, financial, and health sectors. For example, in the financial sector, data sharing pools are prevalent.

---

36 Ibid.
38 Ibid.
39 Ibid.
among digital credit lenders and credit reference bureaus. Builders in fintech also need to take into account laws that regulate the financial sector and protect end users.

Example: The KeHMIS Project

The Kenya Health Management Information System (KeHMIS) project was started in 2011 with the main goal of supporting the Ministry of Health (MOH), health management teams at the county level, and service delivery partners to advance health information system innovations. Given the sensitivity of the data involved, the KeHMIS project is a closed data pool; this model is adopted when there is a heightened need to protect the privacy and security of data. The KeHMIS project supported the development of a National Data Warehouse (NDW), which serves as a centralized repository for anonymized, patient-level HIV clinical care data gathered by health facilities. It contains data for more than 2.2 million patients from over 1,200 health facilities. The NDW also acts as an analytics and visualization platform and it’s used by the MOH, county governments, and other actors to support data-led decision-making and strategic planning. The KeHMIS project also developed an interoperability layer to facilitate data exchange between various health information systems, promoting data sharing and supporting automated reporting.

Based on the above, data sharing pools are suitable for builders striving to fill knowledge gaps by combining data with that of other organizations and drawing on insights derived from these jointly managed repositories. This model allows builders to collectively determine the conditions of use and access to the data.

---

Key questions to answer when setting up a data sharing pool:

- What are the incentives for actors to pool data?
- What type of data is being shared and how does it need to be protected?
- What privacy safeguards (e.g., anonymization or privacy-enhancing technologies) can be used to better enable secure data storage and access?
- How will decisions be made between participants (e.g., about how data is collected, stored, used, and shared)?
- Who will manage the shared data and based on what mandate?
- How will the shared data be used?
- What enforcement mechanisms are in place if sharing rules are breached?

Data commons

Schimowski describes data commons as a “governance model in which individuals collect data and pool it together to produce databases and eventually products or services based on this data that are managed as a common.” ⁴⁵ Commons can be described as community-managed resources governed in the public interest by a shared set of rules. The model is beneficial because it allows data subjects to collect and pool data in a shared database to make it more widely accessible and useful. A good example of a crowdsourced data commons is Wikidata, which is an open knowledge database for structured data maintained by Wikimedia.

Data controllers and processors operate under uniform rules set by members, whose admission may be tied to being a participant and contributing to the data relevant to the membership, regulating particular actors’ rights and obligations, and determining the data processing activities. This makes it easier to observe the common rules related to processing data. Builders can offer services and design products based on the pooled data, whether personal or non-personal. Moreover, individuals can be rallied to generate data — such as health data that previously did not exist — for societal goals.

that benefit the whole community. Importantly, data commons can provide an alternative to the hegemonic control of (and gated access to) data that are commonplace among powerful private (and public) actors.

Obtaining consent to use data and managing conflicts of interest are important challenges related to the operation of a data commons. It may be difficult to decide what data should be made public, especially when it comes to sensitive data, like that held by, for example, a health data commons. Other challenges include managing large quantities of data and tensions over information control between different institutions or actors involved, which could lead to legal challenges, interorganizational competition, and secrecy. To address these limitations, actors who have established data commons tend to allocate a set of rights and obligations about how pooled data is to be treated as a shared resource and the benefits that may be derived and shared between all actors. These are presented as either formal or informal governance rules.

Data commons are often used in health, environment, and crisis and emergency response sectors. Usually, actors need incentives for making their data accessible so all actors can use the shared data. Notably, the data commons model could also help ensure that data is not held in silos by companies that are mainly located outside the African continent so that there is a broader availability of local and regional data for communal use.

The key features for effectively managing data commons are norms of authority and information maintenance, which find expression in Kenya’s Data Protection Act, 2019,


48 Ibid.


and the Data Protection Regulations 2021. Self-organized communities like these require robust governance that gives effect to the rights and obligations of each actor as relates to the commons, and manages and distributes the benefits that may accrue from it.

**Example: Digital Matatus**

In Kenya, the transportation industry is an example of a sector that has fundamentally benefited from the data commons. One relevant case study in this context is the Digital Matatus project, which was pioneered by Kenyan and American universities and the technology sector in Nairobi to fill the gap presented by inconsistent and unreliable transit data in Nairobi. The Digital Matatus project collects and updates data on the matatu routes in Nairobi with the aim of leveraging technology and partnerships locally to enable a more visible, open, service-oriented, and efficient public transport system. By providing free data, maps, and applications to the public, the project has redefined how people navigate the transportation system, spurred innovation, and improved service delivery for the residents. The technology community has also benefited; companies have used the data to develop transit applications and mobile applications that offer route information to the general public. It has also been relevant for the government, which has used the data for city planning and to create a comprehensive visualization of the matatu system in Nairobi.

The Government of Kenya, through the Kenya Information and Communications Technologies Board (now under the roof of the Information and Communication Technology (ICT) Authority), implemented the Kenya Open Data Initiative, which can be viewed as an example of a data commons. By 2016, it hosted more than 800 datasets relating to education, energy, health, population, poverty, water, and

---

51 Matatus are privately owned minivans that transport people from one place to another for a fee.
53 Ibid.
54 Ibid.
55 Ibid.
56 Ibid.
sanitation. The portal led to more than 5,500 dataset downloads (with the data subsequently used in other websites and blogs) and registered 1.1 million visits in 2013. Upon launch, it also included geospatial boundaries for the country’s 47 counties and geocoded datasets.

### Key questions to answer when setting up a data commons:

- What is the source of the data and who controls it?
- Do you have authorization and authentication standards in place? Who has access to the different categories of data?
  - Where different datasets are involved, and especially sensitive data, it is meaningful for builders to categorize the users who have access to these data sets and to attach security and compliance practices. As such, platforms implementing data commons have features requiring digital ID services that grant access controls.
- What type of data do you collect?
  - Some commons may specialize in particular types of data, for example health data, and will therefore have very specific purposes — and security requirements. This kind of information helps builders identify, for example, the restrictions and responsibilities that may be attached to their commons based on the types of data collected.
- Do you have mechanisms in place to govern data management, including rules and agreements for data subjects, controllers, and users?
  - Data Commons have three primary interest holders: the data commons service provider who operates the commons, the data contributor who provides data for the data commons, and the data user who accesses the data. You need agreements to govern the terms for contribution to the commons (data contributors’ agreement) and to access the commons (data access agreement) for each of these interest holders.

---


58 Centre For Public Impact, “The Kenya Open Data Initiative.”

59 Centre For Public Impact, “The Kenya Open Data Initiative.”

Bibliography


http://digitalmatatus.com/.


https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5636009/.


https://kenya.opendataforafrica.org/.


Mazer, Rafe. “Emerging Data Sharing Models to Promote Financial Service Innovation: Global Trends and Their Implications for Emerging Markets,” FSD Kenya, June 1 2018, 

Micheli, Marina, Marisa Ponti, Max Craglia and Anna Berti Suman. “Emerging Models of Data Governance in the Age of Datafication.” Big Data & Society, 7(2). (September 1, 2020)


Rocchi, Giulia and Stefano Lucarelli, “Some Reasons to Think About Big Data as Data Commons.” DECODE, April 12, 2018.

