Module 2: Responsible Data Practices, Governance & Ethics

Inclusion Data Quest

WE ARE OPEN

Module Objective

By the end of this module, participants should be able to:

1. Understand how data is interpreted as a legal concept
2. Understand global and Kenyan data protection principles
3. Differentiate between personal and sensitive data and how to handle it
4. Understand what data protection by design and default means
5. Understanding of data management principles and relevant legal issues, enabling them to effectively and ethically manage data

Agenda

1. Understanding Data Protection and Privacy as Legal and Practical Concepts
2. As a case study, understand the general structure of the Kenya Data Protection Act and fundamental concepts and terms within it
3. Recognizing sensitive data and how to handle it
4. Understand what data protection by design and default means
5. Ethics in data governance practices

1. Understanding Data Protection and Privacy as Legal and Practical Concepts

Data and the Law

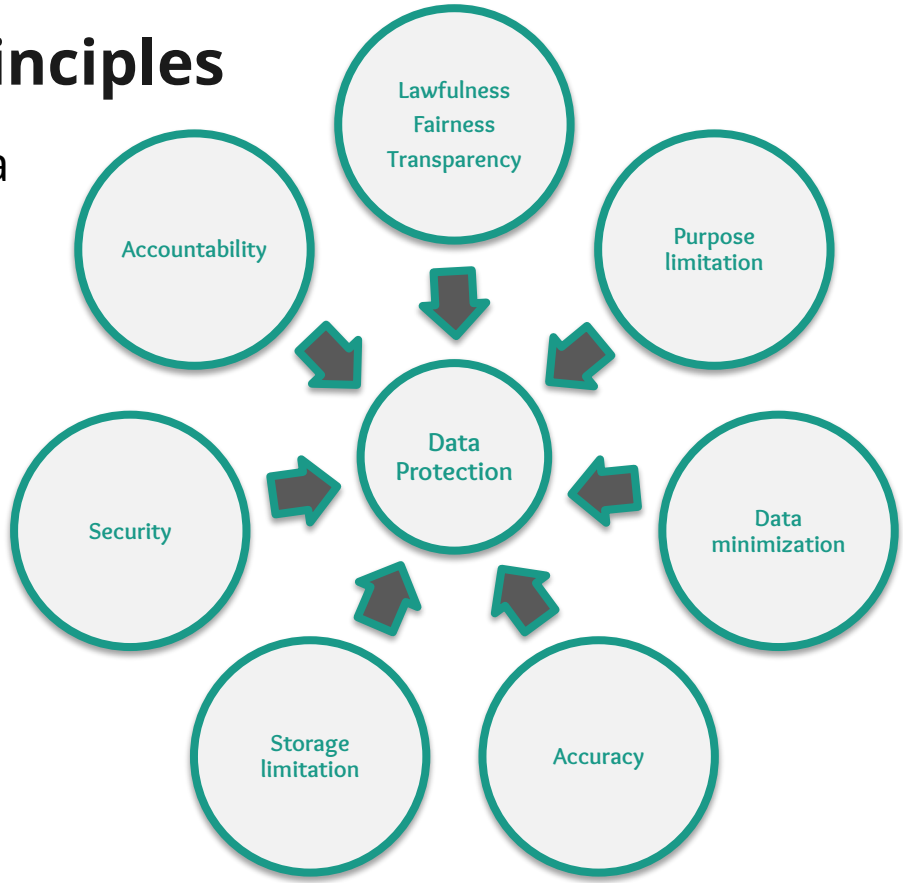
- Data has some characteristics – or attributes – that can make it hard to define in law. A good analogy is a river.
- Like water, data flows. It flows across different devices – laptops, phones, tablets, paper
- Sometimes it is amassed in servers and databases – like water in a reservoir, behind a dam. Streams of data can flow in different directions at different times, just like rivers.
- The fact that data flows can make it hard for the law to keep track of how to regulate it

Kenya’s Data Protection Act 2019

- The DA came into force on 25 November 2019 and is the primary source of data protection law in Kenya.
- The Act gives effect to Article 31 of the Constitution of Kenya 2010 which guarantees the right to privacy and includes the right not to have information relating to family or private affairs “unnecessarily required or revealed” and the privacy of communications infringed.
- Kenya’s DPA 2019 adopts many aspects of the **EU’s GDPR** and in parts, replicates the GDPR word for word.

Data Protection Principles

- Data protection consists of a series of principles. These principles appear in the GDPR in Article 5
- The Kenyan DPA sets out its data protection principles in Part IV section 25 **“Principles of personal data protection”**



2. Breaking down the Kenyan Data Protection Act: Key Provisions

Definitions

- A **data controller** is a person, company, organisation, public authority, or other body, which “alone or jointly with others, determines the purpose and means of processing personal data”.

- A **data processor** is a person, company, organisation, public authority, or other body, which “processes personal data on behalf of the data controller”.

- Other relevant information:
  - In the Act, the data controller must engage a data processor that provides sufficient guarantees that organisational and technical measures are in place to keep personal data safe and there **must be a written contract that sets out the data controller’s instructions.**
  - Data controllers and data processors must establish **data retention schedules**, which state the reasons for keeping personal data, how long it will be kept for and when retention will be reviewed.

Definitions

- ‘processing’ of personal data essentially means the use of personal data.
- In the Act, all the shown actions are considered processing:

adaptation alteration available collection combining consultation destruction disclosure dissemination erasure making organisation otherwise recording restricting retrieval storage structuring

Data Protection & Privacy

Data protection by contrast is about how data that might be able to personally identify you as an individual or expose sensitive information is safeguarded.

The **right to privacy** is a universal human right, established by the Universal Declaration on Human Rights and elaborated on in many international laws and also many national laws

Personal Data

- Personal Data is defined in the Act as “any information relating to an identified or identifiable natural person”. An ‘identifiable natural person’ is a person “who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity”.
- This is identical to the wording that is found in Article 4(1) of the GDPR/UK GDPR

Sensitive Data

- Sensitive data is personal data that requires extra care when processing because of its nature.

- The DPA defines it as:

"Data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject".

Discussion

- Is there data that your organization collects that might be considered ‘personal data’? Please describe it and its attributes.
- Do you really need to collect it?

Protecting Personal and Sensitive Data

There are two main ways that individuals can claim legal rights over information about them.

a) The first is by exerting their human right to privacy - in Kenya this is a Constitutional right of every Kenyan citizen.
b) The second is by regulating how personal or sensitive data is controlled by the various people who have a responsibility to look after it as “data controllers” and those tasked to “process” or “data processors”

Privacy (vs Security)

- Data privacy refers to the protection and control of personal data, ensuring that individuals have the authority to determine how their personal information is collected, used, stored, and shared.
- It involves safeguarding sensitive information from unauthorized access, misuse, or disclosure.

Data Privacy

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete the data

≠

Data Security

Measures that an organzation is taking in order to prevent any third party from unauthorized access.

Consent

The Kenyan Act contains ‘conditions for consent’ that replicate those found in the GDPR.

The GDPR dictates that for consent to be valid it must be:

- Clearly distinguished.
- Intelligible.
- Easily accessible.
- Freely given.
- Specific.
- Withdrawn if desired.
- It is not possible to make a contractual term conditional on consent for processing personal data for other purposes.

Data Transfers

- The legal conditions for transferring personal data to another country are found in Part VI, section 48 of the Act.
- The transfer is necessary if:
  - It is necessary for a contract with the data subject.
  - For a contract that is in the interest of the data subject between the data controller and another person.
  - For any matter of public interest.
  - For the establishment, exercise or defence of a legal claim in order to protect the vital interests of the data subject or of other persons, where the data subject cannot give consent.
  - For a compelling legitimate interest pursued by the data controller or data processor that are not overridden by the interests, rights and freedoms of the data subject(s).

Reflection

What concepts stand out for you in this discussion regarding the DPA?

3. Ethics in data governance practices

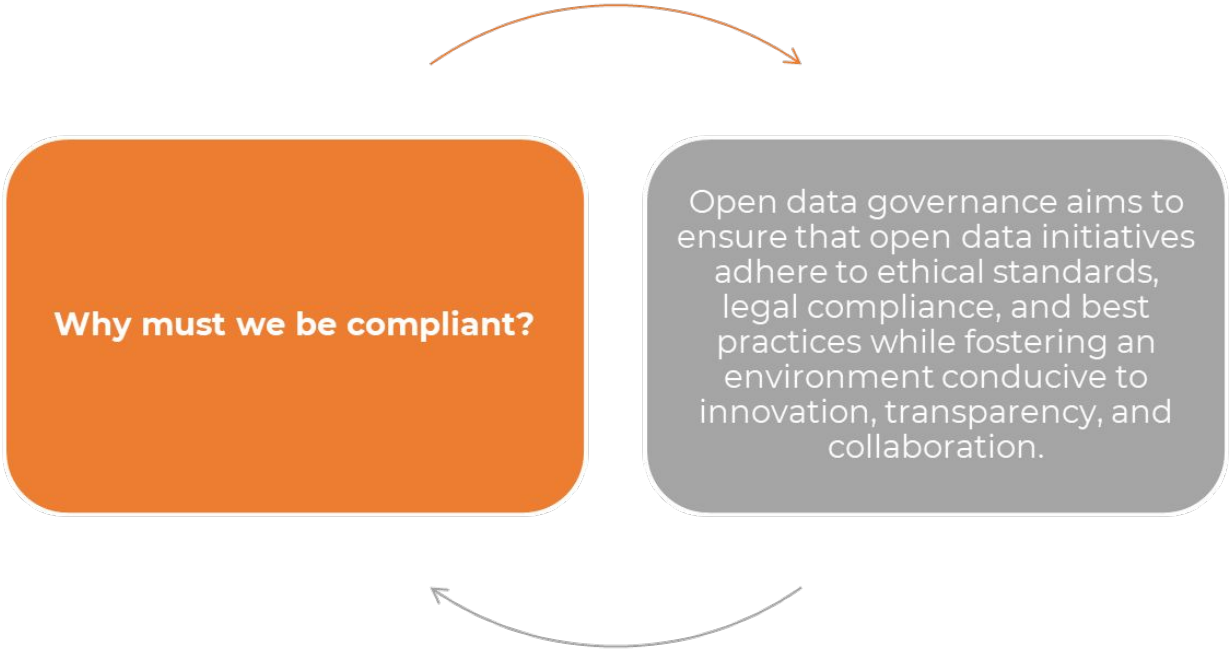
Discussion

A government health agency has collected a large dataset containing anonymized patient health records, including medical conditions, treatments, and demographic information.

The agency intends to make this dataset openly available for research purposes to promote scientific advancements and improve healthcare outcomes.

1. What measures or strategies can be implemented to address the security and privacy concerns while still promoting data openness?
2. What ethical considerations need to be taken into account?
3. How can stakeholders, such as researchers, healthcare providers, and patients, be involved in the decision-making process to strike a balance between openness and security/privacy?

Definitions - Data Governance & Ethics



Definitions

Open data governance refers to the set of **principles**, **processes**, **policies**, and **structures** put in place to manage, oversee, and facilitate the sharing, accessibility, and usability of open data.

It involves the management of data to ensure its quality, accessibility, security, and ethical use while promoting transparency and maximizing its potential benefits to various stakeholders.

Definitions - Foundations for data governance

- CARE Principles complement the FAIR Principles and are implemented in the data lifecycle
- These principles ensure that data is accurate, reliable, secure, and accessible when needed.

Current Challenges in the Information Society impacting electronic access/sharing of data

Data Governance & Management Principles-1

Policies and Standards:

Establishing clear policies, guidelines, and standards for data collection, storage, sharing, and usage. These policies define the scope, quality standards, licensing, metadata requirements, and other aspects necessary for consistent and effective data management.

Data Stewardship and Ownership: Defining roles, responsibilities, and ownership of open data within organizations or initiatives. Assigning data stewards who oversee data management, ensuring accountability and proper governance.

Transparency and Accessibility: Promoting transparency by making data sources, methodologies, and updates easily accessible. Ensuring that data is available in open formats and through user-friendly platforms to facilitate access for stakeholders.

Data Governance & Management Principles-2

Quality Assurance: Implementing mechanisms to ensure the quality and reliability of open data. This involves regular assessment, validation, and maintenance of data to uphold its accuracy and relevance.

Security and Privacy: Addressing security and privacy concerns by implementing measures to protect sensitive information and prevent unauthorized access or breaches.

Engagement and Collaboration: Encouraging collaboration among stakeholders, including government agencies, organizations, researchers, and the public.

Evaluation and Improvement: Continuously evaluating the effectiveness and impact of open data initiatives. Gathering feedback, assessing outcomes, and making necessary improvements to governance structures to enhance data utilization and benefits.

What is Legal and what is Ethical?

- Legal issues include compliance with data protection and privacy laws, intellectual property rights, contractual obligations, and regulatory requirements.

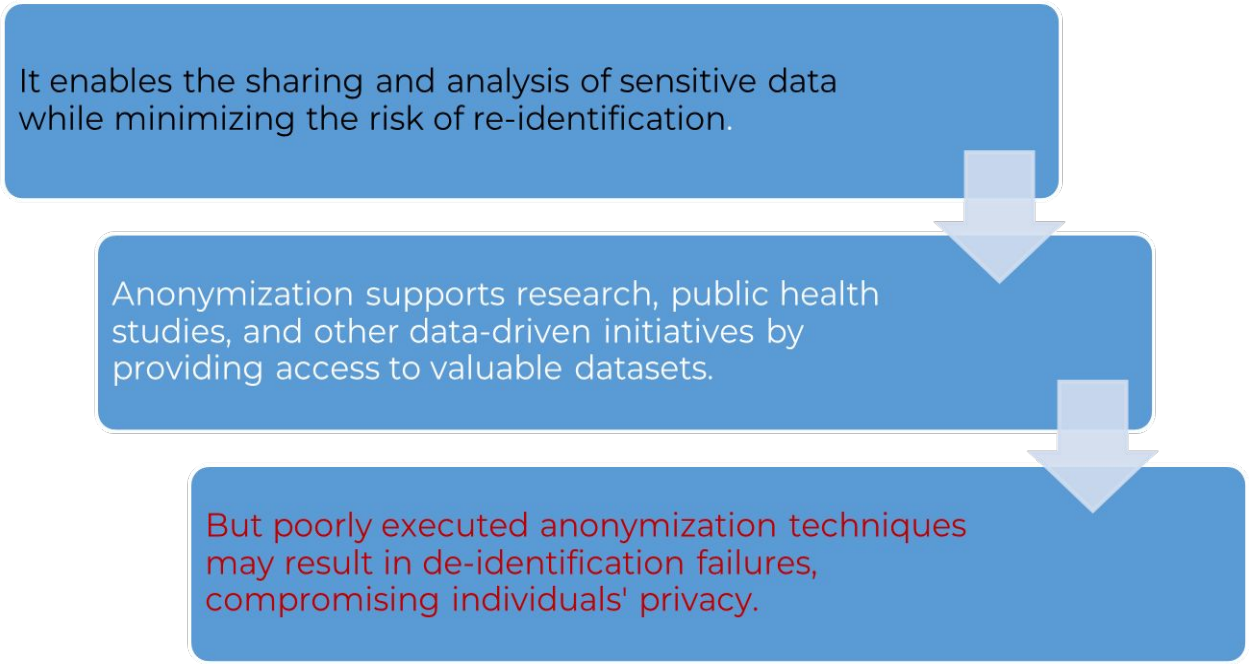
- **Ethical issues encompass ensuring informed consent, protecting individuals' privacy, minimizing bias and discrimination, and promoting transparency and accountability.**

Ethical Considerations in Data Management - 1

Informed Consent	Obtain informed consent when collecting personal data, ensuring individuals understand how their data will be used and have the option to opt-out.
Fair Use and Non-Discrimination	Ensure fair and equitable access to data.Avoid discrimination or bias in data collection, sharing, and analysis to prevent unfair outcomes.
Respect for Cultural Sensitivities	Consider cultural norms and sensitivities when sharing data, especially regarding indigenous or local knowledge, ensuring respect for traditions and values.
Accountability and Integrity	Maintain data accuracy, prevent misuse, and hold individuals or entities accountable for ethical violations. Implement measures to detect and address unethical practices

Ethical Considerations in Data Management - 2

Anonymization is the process of removing or obscuring information from a dataset that could be used to identify individuals, households, or businesses, so that their anonymity is preserved and protected



Balancing Openness with Security and Privacy

Risk Assessment and Mitigation: Conduct risk assessments to identify potential vulnerabilities and threats to data security and privacy. Implement measures to mitigate risks, such as encryption, access controls, and regular security audits.

Data Protection Measures: Implement robust data protection measures, including encryption, data minimization, secure storage, and controlled access, to safeguard against unauthorized access or breaches.

Contextual Openness: Assess the level of openness needed for each dataset. Not all data may require complete openness; some might need restricted access based on sensitivity or security concerns.

Transparency in Security Practices: Be transparent about security measures in place to build trust with stakeholders.

Compliance with Legal and Regulatory Frameworks: Ensure compliance with relevant laws and regulations governing data protection, privacy, and security, both nationally and internationally.

Case study: Lessons from Kenya National Bureau of Statistics

Ethical considerations:	Be transparent in why you are collecting the data.
	When interviewing individuals, obtain consent
	Safeguard data and respect the privacy of your respondents
	Abide by the laws and regulations of the area of data collection
Clarity and Quality:	Use plain language and avoid double barrelled questions
	Data entry - Validate data and check data accuracy
	Use numerical codes where possible to handle qualitative data entry
	Avoid mixing data types (text and numerical)
	Consistently handle missing values
Documentation:	Keep a record the data collection/generation process. This helps the data producer remember the details on how the data was generated

Key Takeaways from Module 2

- Data is regulated through control and processing (not ownership), focusing on privacy and flow management. Kenya's DPA and GDPR emphasize roles of *data controllers* (decision-makers) and *data processors* (implementers).
- Both GDPR and Kenya's DPA prioritize **lawfulness, transparency, and accountability**, with penalties tied to violation severity
- **Personal data** (e.g., name, address) identifies individuals, while **sensitive data** (e.g., health status, race) requires stricter safeguards. Processing sensitive data demands explicit consent or legal justification.
- Privacy must be embedded in systems from inception. **Data Protection Impact Assessments (DPIAs)** are mandatory for high-risk activities (e.g., large-scale processing or biometric data use).
- Ethical governance balances **openness** (e.g., FAIR/CARE principles) with **security** (anonymization, encryption). It requires transparency, cultural sensitivity, and compliance with laws