Study Unit 4

Introduction to Regulatory Framework

Introduction

The emergence of the Internet as a global telecommunications network has had a huge impact on how we view and apply data protection and regulations. Before the massive expansion of the Internet, data was a minority interest that did not generate significant global interest. However, over the past decades, the use of and processes for data evolved significantly — both in terms of technology and use cases. Data is now considered the raw material for digital transformation. Thus, there is a need for a form of regulation to avoid chaos and misuse.

This Study Unit will provide you with an understanding of what a regulatory framework is and what it is used for. You will learn about general data protection principles including your country's data regulations. Likewise, you will get to know why we need FAIR data policies and its benefits to your country. Finally, the basics of a FAIR policies will be explored.

Learning Outcomes of Study Unit 4

Upon completion of this study unit, you should be able to:

4.1 Discuss and explain the legal and regulatory frameworks and the key concept of Data regulation framework.

4.2 Summarize Data Protection law and explain what GDPR is and its principles.

4.3 Describe the FAIR Data Policies.

4.4 Define Data Protection Laws in specified countries.

4.5 Explain the FAIR compliance with Data.

4.6 Discuss the Privacy and Data protection laws in implemention countries

Introduction to Regulatory Framework Outline

- Regulatory Framework
- Key concepts of Data Regulatory Framework
- GDPR and its principles
- Data Regulation specific to Sudan, South Sudan, Somalia and Ethiopia
- FAIR Data Policies

Study Unit Duration

This Study Session requires a 4 hours of formal study time.

You may spend an additional 2-3 hours for revision

4.1 Introduction to Regulatory Frameworks

In 2017, The Economist released an article with the topic “The world's most valuable resource is no longer oil, but data" , reflecting the transformation of our modern economy, where massive data collection and analysis has become a key competitive advantage. As data becomes an important part of our lives, regulations on data and data protection becomes inevitable.

While dealing with any type of data, whether on the national or international level, there are many things that have to be considered. Examples are data protection laws forming the regulatory framework on how to obtain, use and store data.

4.1.1 Legal and Regulatory Frameworks

A good legal and regulatory framework is essential for the effective administration, operation and maintenance of any system. Good legal and regulatory framework clearly defines the roles and responsibilities of all parties involved.

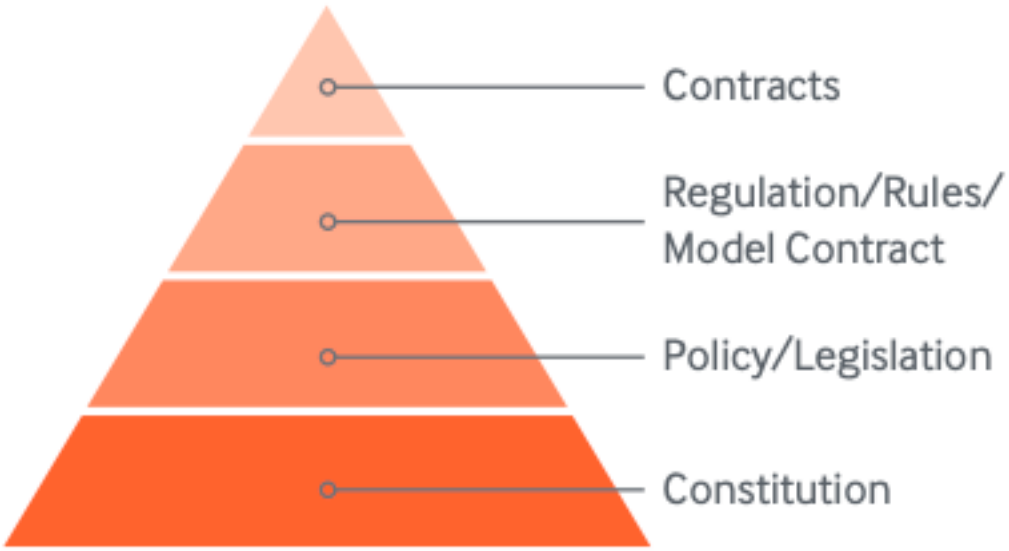

Figure 4.1: The Legal Hierarchy, Source: NRGI

Moving from the base of the pyramid to the top, each tool becomes more detailed or specific. Each instrument on the pyramid must correspond to the instruments below it. In a well-ordered legal

hierarchy, a country will not agree to terms of a contract that conflict with rules set out in regulations, legislation or the constitution. In addition, laws and policies should have more authority than a contract - from a legal point of view has priority. However, in practice, contracts can also be drafted in such a way as to explicitly defy laws and regulations.

Difference between legal and regulatory framework

	Countries are strongly encouraged that the law sets out general principles for civil registration, while using regulations to regulate operational and technical aspects.

What is Regulatory Framework?

Regulations can be defined as the management and organization of systems according to a set of rules. There are rules for all areas of our daily life. Moreover, rules are also present in business and in all kinds of political systems. In this module, we will study the Regulatory Frameworks of data, data protection and privacy issues in Sudan, South Sudan, Ethiopia and Somalia. First of all, let's understand what is Data Regulatory Framework.

Definition of Data Regulatory Framework
Data Regulatory Framework means any laws, regulations, rules and policies officially developed and approved by the government, for the purposes of regulating data sharing, data privacy, data protection and any issues related to data. The spirit of regulation is to establish fairness and openness, and thus, being drivers of innovation.

Why do we need it?

A good regulatory framework is significant for the effective management, operation and maintenance of data within the country and therefore, serves for the greater decision-making. A proper legal framework clearly defines the roles and responsibilities of all stakeholders involved in data curated issues. Thus, a regulatory framework is a model people can use for reforming and enacting regulations in an effective and logical way.

Evolution of Data Regulations

Prior to the data protection reforms undertaken in many countries during the last decades, history of protection of sensitive data started a long time ago. This includes medical data, mental health-related data, financial data, personal data (religious beliefs, political affiliation organizational membership, racial or ethnic origin), genetic data, biometric data and etc.

As more and more social and economic activities take place on the Internet, the importance of privacy and data protection is becoming more evident. The collection, use and sharing of personal information to third parties without the notification or consent of consumers are also of concern.

Data Protection and Privacy Legislation Worldwide

New and updated national data privacy and data localization laws are fundamentally altering the way that companies can conduct businesses internationally and within countries. Up to 2020, 132 out of 194 countries have enacted data protection and privacy legislation throughout the world. Data Protection and Privacy Legislations are registered in Sudan, Ethiopia, however not registered in South Sudan and Somalia.

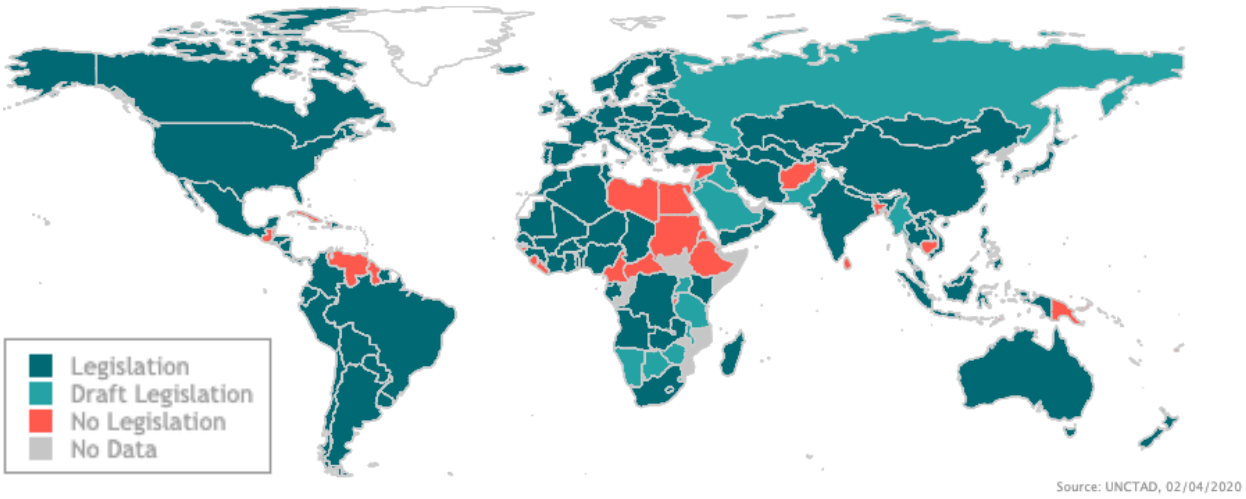

Figure 4.2: Data Protection and Privacy Legislation Worldwide up to 2020.

Benefits of Data Regulations

1. Increases the transparency in the data processing
2. Improves consumer confidence
3. Better data security
4. Greater decision-making

Peer to Peer Interaction

Do you think Regulatory Frameworks are important?

Why do you think they are important? Explain this to your peers

4.1.2 Key concepts of Data Regulatory Framework

When we talk about the Data Regulatory Framework you must also understand these concepts:

Data Protection

Data protection is the process of safeguarding confidential information from corruption, compromise, loss or breach. The importance of data protection has increased since the amount of data created and stored are continuing to grow. Therefore, developing such policies and regulations that include data protection is extremely important these days.

Data ownership

Data ownership is the existence of legal rights and complete control over an individual piece or set of data elements.

Examples of data ownership in different regions:

US: Data belongs to the company or organization who has the data

China: The state is a guarantor for data re-use

Europe: Data belongs to the Data Subject (GDPR)

Data Security

Personal information must be stored and processed securely and protected from unauthorized or illegal processing, loss, theft, destruction or damage.

- **Defining Personal Data and Sensitive Personal Data**

  Fundamental elements of any data policy framework are the definitions of **Personal data** and **Sensitive Personal Data**.

Definition of Personal Data
Personal data is any data that can reasonably be linked or are associated, directly or indirectly, with a certain individual.

Definition of Sensitive Personal Data
Sensitive personal data is personal data consisting of ethnicity, political affiliation, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sexual orientation, some known data minors and accurate geolocation data.

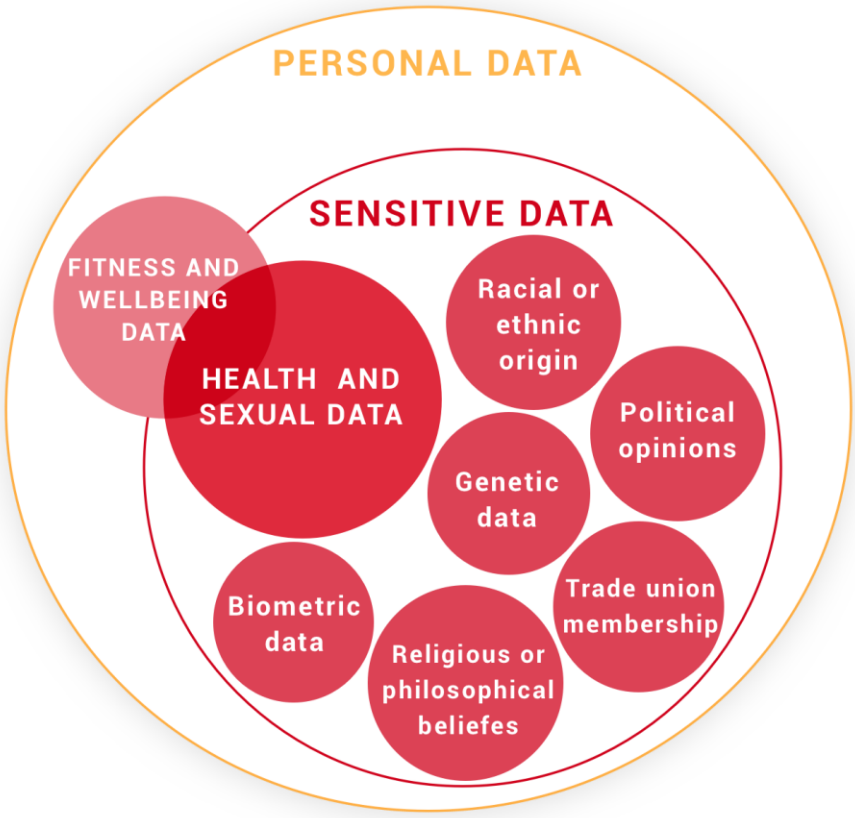

Figure 4.3: Shows Fundamental elements of any data policy framework
Source: https://www.chino.io/compliance/gdpr-compliance-health-applications

- **Definitions of Encrypted, Anonymized and Pseudonymised Data**

  Encryption of personal data – encryption is a mathematical function that encodes data in such a way that only authorized users can access it.

  Pseudonymization of personal data - helps to reduce privacy risks by making it more difficult to identify individuals. Pseudonymization means that a person can still be identified using indirect or additional information.

  Anonymization of personal data - anonymization is the process of removing **personal** identifiers, both direct and indirect, that may lead to an **individual** being identified. You completely lose the connection between data and the individual.

	With anonymization, the data is cleared of any information that could serve as an identifier for the data subject. Pseudonymization does not remove all identifying information from the data, but simply reduces the ability to associate a dataset with the original identity of a person. Thus, no individuals can be identified from those data without a "key" that allows the data to be re-identified.

Data sharing

Since linking information between databases increase concerns about privacy and data protection, the legal framework can reduce risks by defining all the purposes for which personal data are used by both state and non-state organizations.

Cross border data transfers

This is also one of the key concepts of Legal Framework. However, because of uncertainty regarding data protection standards in foreign countries, many countries limit transfer of personal data across borders. This is particularly sensitive in the case of personal data.

User consent and control

One of the generally accepted principles of confidentiality is that a person's personal data should be collected and used only with the consent of that person, unless otherwise provided by law for such collection and use.

Peer to Peer Interaction

Have you encountered any of these concepts before this module in your life? If yes, specify them

4.2 Data Protection Law

Add content here

4.2.1 Data ownership

US Model: data belongs to the company who has the data;

Chinese Model: the state is the guarantor of data re-use;

European Model: the data belongs to the data subject;

4.2.2 Data protection

The historical concept of privacy can be understood across several centuries of legislation. It began to take firm shape in 1948, in the Article 12 of the Universal Declaration of Human Rights: “No one will be the object of arbitrary interference with his private life (...). Everyone has the right to be protected by the law from such interference or attacks"

The regulation for the protection of personal data is very recent phenomenon. This is directly related to the development of information technology and the increase in data collection by organizations.

Now that data is mostly stored in a digital format, storing and protecting it becomes very important. The collected data must be properly stored and strict rules must be followed to ensure the security of data.

Figure 4.4: Shows Legal foundations in Europe

4.2.3 European Data Regulatory Framework - GDPR

The General Data Protection Regulation (GDPR), which went into effect in May 2018, is a European Union regulation. However, because its requirements apply broadly, in general, any organization that does business in the European Union in some way or interacts with European Union citizens, the GDPR matters to many companies outside of the European Union. A Data Subject is a central point in this regulation where data belongs to a Data Subject and who has the rights whether to give permission to use his data or not. The GDPR does not apply to anonymised information.

4.2.4 Key terms of GDPR

Data Controller is a person, company, or other body that determines the purpose and means of personal data processing. Putting it simply, the data controller will be the one to decide how and why data is going to be used.

Data Processor – A person or organization who deals with personal data as instructed by a controller for specific purposes.

Data Subject is an identified or identifiable natural person, has to be a person (not a company or organization). Person can be identified using available data markers, including elements such as names and unique identification numbers.

4.2.5 Applications of GDPR

- To organizations within the EU and to any external organization that is trading within the EU;
- Data controller and data processor can be found in breach;
- The regulation protects all-natural persons whatever their nationality or place or residence;
- Applies to all people residing in the EU and to non-European citizens as well (including refugees, migrants)

4.2.6 GDPR Data Protection Principles

Personal Data shall be:

1. Processed lawfully, fairly and in a transparent way in relation to the data subject
   i. Lawfully
      - Satisfy a lawful basis
      - Not breach other laws or be unlawful
   ii. Fairly
      - ➢ Ways people would reasonably expect
      - ➢ Is not harmful or misleading
   iii. Transparently
      - ✓ Clear, open and honest

2. Purpose limitation

Collected for specific, explicit and legitimate purposes and are not further processed in a manner incompatible with these purposes.

a. Data minimization – adequate, relevant and limited to what is necessary
b. Adequate – sufficient amount

c. Relevant – links to the purpose
d. Limited – no more than you need
e. Accuracy – accurate and, where necessary, kept up to date
f. Storage limitation – stored in a form that allows the identification of the data subjects for no longer than necessary
    - Determine how long you need it
    - Periodically review what you hold
    - Erase or anonymize when longer needed
g. Security principle – data is protected from unauthorized or illegal processing and accidental loss, destruction or damage

Accountability

The controller responsible for and able to demonstrate compliance with the principles above given

Peer to Peer Interaction

Discuss with your peer the difference between Data Subject, Data Controller and Data Processor.

4.3 FAIR Data Policy

With a fast growing and evolving data environment, and new technologies and more complex data types, it is now more important than ever for data to be machine-actionable. Harmonizing and integrating data stored in general and special purpose repositories, making such data Findable, Accessible, Interoperable and Reusable, will help in maximizing the value of it, saving time, and significantly reducing research costs and its outcomes.

To begin, technology must be underpinned by legal frameworks that safeguard individual data, privacy, and user rights. When it comes to FAIR Data, acceptance and successful deployment includes the development of regulatory obligations in a manner that privacy and security of data are guaranteed and compliant with the national data policies.

4.3.1 Definition of FAIR Data

You have already learned about the FAIR principles from the previous modules, but, in summary, FAIR stands for Findable, Accessible, Interoperable, Reusable. This is a set of guiding principles that do not force data producers to adopt any particular standards or technologies. It encourages to think about the broader picture of where their data is in the broader context and how it can be optimized for impact and longevity.

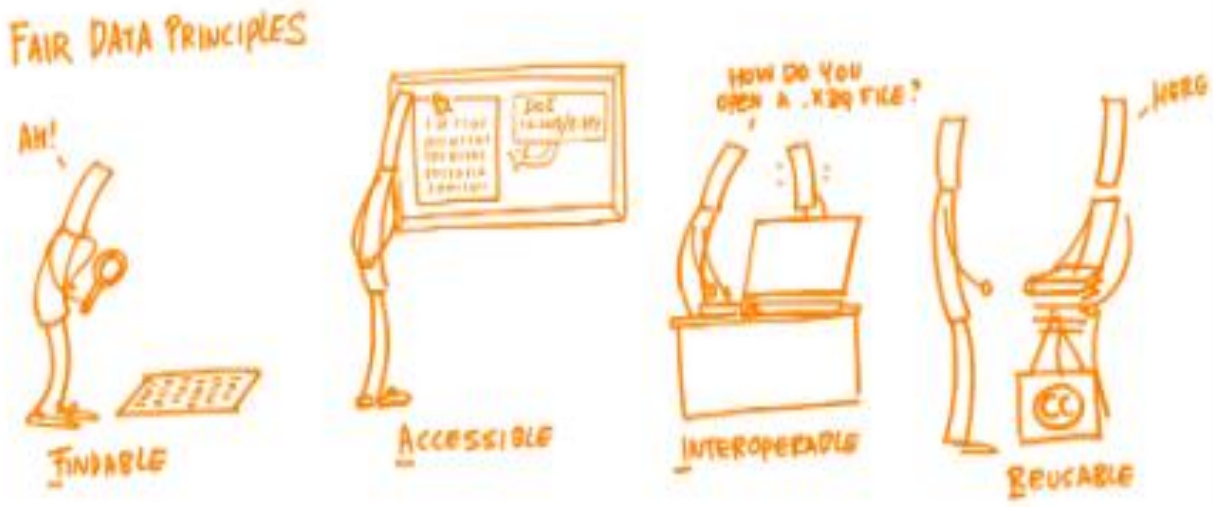

Figure 4.5: Shows the fair data principles

Source : https://www.fosteropenscience.eu/learning/open-and-fair-research-data/#/id/5e3741af3ccdf1010dbc6f26

4.3.2 FAIR DATA does not equal to Open Data

A common misconception is that FAIR-compliant data must be open at the same time. This is definitely not the case, and a common phrase used in the open research community is "open as much as possible, closed as necessary." There are many examples where data cannot be opened by default, such as data subject to intellectual property rights and sensitive data. On the other hand, Open Data is in open format that can be freely used, re-used and shared by anyone for any purpose.

When people talk about Open Data, they mostly mean Open Government Data which are produced by the public sector. However, there is also open data produced and released by private companies such as Netflix, Uber, Lyft and others. For instance, Netflix opened some of its data to a competition that could create a better algorithm for offering films to Neflix viewers. Lyft and Uber have released some of their data to study the impact of transport companies on traffic. Apart from such data, we must also take into account data provided by public or private companies while carrying out research or patient data that is produced by healthcare organizations. Such data may not always be open to legitimate business interests or for security or privacy reasons, but they can and should always be FAIR.

4.3.3 FAIR as a service based on the legal and regulatory framework

The growing importance of issues related to the growing volume of data and access to it makes the work of data harmonization, as well as the creation of data policies, extremely important. FAIR policy shaping is required for good data management practice. Therefore, this can lead to the implementation of additional data policies on FAIR.

Information from a wide variety of areas, including technical, ethical, security, legal, cultural, behavioral and economic, must be gathered in order to inform a guideline directed towards providing the optimal strategy to implement a FAIR data policy.

By definition, to be FINDABLE, any data object should be uniquely and persistently identifiable; a data object is ACCESSIBLE by machines and individuals under the conditions explained in the policy; data use a formal, accessible, shared, and broadly applicable language for knowledge representation in order to be INTEROPERABLE; the data object has a plurality of accurate and relevant attributes (usage license, provenance, community standards) to be REUSABLE.

4.3.4 Benefits of FAIR Data policy

Having FAIR data policy with data in well-defined formats has many benefits:

- It makes previously measured data available for further analysis without the necessity to repeat the experiment.
- It promotes data use, interdisciplinary research and the widespread use of Artificial Intelligence.
- Data becomes accessible to other researchers, which ensures scientific integrity and reproducibility of experiments.
- Scientists can explore data in previously unknown ways or reapply new methods to existing data.

4.4 Data Protection Law per country (contextualization)

Without analyzing each national law, an analysis of initiatives implemented on a regional scale provides a holistic view of the main trends in privacy. Therefore, we will go deeper into the Data Protection Law of your country of residence.

4.4.1 Data Protection Law in Ethiopia

The Government of the Federal Democratic Republic of Ethiopia has put in place laws and legislation to promote access to online data and information as well as to ensure data protection.

One of such proclamations is the National Data Protection Law, Freedom of the Mass Media and Access to Information (Proclamation No. 590/2008), E-commerce Law, Computer Misuses and Cybercrime Law and the E signature Law. The enactment of these laws provides for the availability of data in open formats while safeguarding the privacy and security of institutions and individuals.

Law

Although the right to privacy is enshrined in the Ethiopian constitution, the current laws do not provide full protection to this right, especially in the realm of personal data. While Ethiopia circulated a draft comprehensive data protection law in 2009, the past decade has seen no implementation of such a law.

Personal Data

The Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, which applies to public bodies, identifies the following categories of information about an identifiable individual as *personal data*:

- Medical, education, academic, employment, financial transaction, professional or criminal history;
- Ethnic, national or social origin, age, pregnancy, marital status, color, sexual orientation, physical or mental health, wellbeing, disability, religion, belief, conscience, culture, language, or birth;
- An identification number, symbol, or other identifier assigned to the individual, address, fingerprints, or blood type;
- Opinions, views, or preferences, except as they relate to another individual
- Views or opinions on grant proposals, awards, or prizes granted to another individual, provided such views or opinions are not associated with the other individual's name;
- Views or opinions of others about the individual; or
- An individual's name, in combination with other personal data, or alone, if it could reasonably be linked to personal data. (An exception applies for persons deceased for more than 20 years.)

Data Protection

The current legal framework is fragmented. Access to information is guaranteed by the Constitution and different ministries, departments and agencies have made an effort to make data online. Article 29 of the Federal Democratic Republic of Ethiopia guarantees a right to obtain information about the activities of state organs and organs of local administration [National Open Data Policy of The Government of Ethiopia (2018)].

The government has also enacted its first Freedom of Information law: The Proclamation to Provide for Freedom of the Mass Media and Access to Information. The Proclamation provides that all persons have the right to seek, obtain and communicate any information held by public bodies, except exempted information therein. Under the Proclamation, citizens have a right of "access, [to] receive and import information held by public bodies, subject to justifiable limits based on overriding public and private interests".

Collection and Processing data

Personal data must be collected and processed with due care and only for an intended lawful purpose. Consent up on collection of personal data is required. There is also a need to have an ethical clearance from government authorities.

Registration and Enforcement

There is no data protection authority or scheme for registration of data controllers.

Cross Border Transfer

Personal data transfers must occur for an intended lawful purpose with the prior written consent of the data subject.

Security and Breach Protocol

The Computer Crime Proclamation No. 958/2016 mandates that service providers implement reasonable and necessary security measures to protect confidential network data from unlawful and unnecessary access. Upon the discovery of a breach, they must immediately notify the Information Network Security Agency and the police, and take appropriate steps toward rectification.

4.4.2 Data Protection Law in Somalia

Somalia does not have any data regulation laws in place. However, the government is on course to create these laws which will be integrated with different 'data management systems from government and partner-led social protection and emergency initiatives.' The integration will assist in the coverage and assessing the impact of social protection programmes as well as help integration of the available data by different sectors of the government. These will be realized by the raft of proposals put in by International Non-Governmental Organizations (INGOs) and Non-Governmental Organizations (NGOs) in the country, meant to improve health, education, cash transfer programmes as well as other social functions in the country. Some of the areas currently covered are:

Data Registration

Since there is no guideline on registration of personal data, most of the agencies have had to develop mechanisms of registering the eligible persons. Some of the notable frameworks in place are:

1. Development of an operational guidance and a toolkit that provides a set of standards and best practices for implementing of programmes and can be deployed in emergency contexts. The toolkit imparts knowledge and the guiding principles of humanitarian agencies for cash transfer programmes in urban areas. The guideline was developed by UNHCR and Cash Learning Partnership.
2. The International Committee of the Red Cross (ICRC) also has a similar guideline which is used to establish the agency's database and manage registration of data in all their work throughout the country.

Data Sharing and Protection

Like data registration, data sharing and protection is the sole responsibility of the agency with the data. This provides a gap for misuse of data collected as the owners of the data are not assured any protection by state. Fortunately, there some existing guidelines for the agencies to avert such unethical behavior. These include:

a. Development of guidelines on data protection. These guidelines also include seeking of consent to share data where appropriate, feedback and complaints handling mechanism and

use of alternative identification documents in cases state sanctioned identification documents are missing.

b. Selection and sharing of eligible persons data based on geographical targeting and community-based targeting.

In geographical targeting, the agencies identify a location for eligible persons based on the classification of need. These needs are ranked in different categories. For example, in the identification of persons eligible for cash transfer focus is usually on different levels based on crisis, emergency and famine. Community-based targeting on the other hand relies on the community members to select eligible persons for the humanitarian programmes in their areas. This is premised on inability of the agencies to conduct an analysis of the levels of need or vulnerability and the fact that a better understanding of the situation can be provided by the community members better than any other outsider.

Within the country, village relief committees (VRCs), Internally Displaced Persons (IDPs) camp committees and the local authority are responsible for data sharing and protection to the different agencies. They are usually elected or self-appointed (apart from local authority and clan elders) based on the power matrix in a location/ camp, also known as "gatekeepers"- sophisticated networks of interference who position themselves to benefit from humanitarian aid for personal gain or political mileage.

4.5 FAIR compliance with data regulatory frameworks in Implementation Countries

4.5.1 Ethiopia

The FAIR guiding principles define the Findability, Accessibility, Interoperability, and Reusability of data stored in different repositories across different geographical locations and disciplines. However, the silos of research data, patient data, and other digital resources resided in either local or cloud repositories have become a nightmare for both machines and humans. Making

data FAIR would realize automatic discovery and analysis of data by machines and ultimately by humans.

It is seldom possible to find the four principles together in the policies, strategies, declaratives, plans, and other regulatory frameworks except for a recently released national open data policy of the government of Ethiopia which includes terms with similar intentions as the four FAIR principles. These documents often mention the principles separately; Findability and Accessibility often appear in information roadmaps and strategies. Interoperability and use of data were also given due emphasis in eHealth Architecture documents and data sharing polices.

The regulatory framework documents used certain vocabularies or phrases that carry similar intention as the FAIR Principles. For example, keywords such as, integrate, harmonize, coordinate, incorporate, collaborate, shared data or services, and information exchange all relate to interoperability. The term **'FAIR-Equivalent'** was therefore coined to designate such terms and statements.

Different sectors have different regulatory framework documents which enable them to govern their activities properly. The following table shows FAIR-Equivalent terms that are included in selected regulatory framework documents in different sectors in Ethiopia.

Sector	**Regulatory Framework**	**Findability**	**Accessibility**	**Interoperability**	**Re-usability**
Ministry of Health (MOH)	Information Revolution Roadmap II (2020)	-	Access, Accessibility, Use of health data,	Interoperability, Harmonization, Alignment, Integration, Linkage	Standardized
Ethiopian Public Health Institution (EPHI)	Ethiopian Public Health Institute Guideline for Data Management and Sharing (2016)	-	Accessed, Accessibility, Use of data, Obtaining	Coordinated, Share data, Integrate	Standardized

Ministry of Innovation and Technology (MInT)	Digital Ethiopia 2025, A digital strategy for Ethiopia inclusive prosperity (2020)	-	Open-access data, access to Information	Aggregate, Interaction, Data sharing, Integrate, Interoperable platforms, Data exchange	Standardized data
Ministry of Communication and Information Technology (Now it is called MInT)	Consultation on the Recommendations and Working Text of the National Open Data Policy of The Government of Ethiopia (2018)	Data to be traced, National Public Key Infrastructure (PKI) framework	Access	Interoperability framework, Integration Systems	Open license, reuse, redistribute, Standard

4.5.2 Somalia

Despite the loads of data taken and shared by different players in the country, there is no existing framework to guide on the Findability, Accessibility, Interoperability and Reusability (FAIR) of the data. Lack of these frameworks create dependence on the "gatekeepers" and agencies expertise for data protection and sharing, which at times maybe compromised.

Therefore, the government and the INGOs and NGOs are currently in engagements that will come up with frameworks that will:

a) Facilitate data sharing and reuse by:
   - Organizing and governing data sharing initiatives in specific communities of practice.
   - Fair and impartial assessment of requests for data sharing

b) Keep design choices in mind by:
   - Explicating, formalizing and continuous updating of data and metadata standards
   - Additional methodological checks, statistical innovations and active monitoring and correction of inadvertent biases

- Ongoing vigilance and transparency when reusing data

c) Respect participants' rights:

- Developing frameworks and methods for privacy and data protection "by design"
- New governance frameworks capable of fostering trust and participation

d) Value data sharing:

- Frameworks and metrics for justifying the value of investments in systematic reuse and sustainable infrastructure
- Systems for scientific credit for reuse which do not reproduce current "publish or perish" reward systems

4.6 Privacy and Data Protection Laws in Implementation Countries

4.6.1 Privacy and Data Protection Laws in Ethiopia

The Constitution of the Federal Democratic Republic of Ethiopia has recognized the right to privacy as a fundamental human right. the country does not have a legally binding comprehensive data protection law. There are several laws that are relate to privacy and data security, including the 1995 Constitution of the Federal Democratic Republic of Ethiopia, the 2005 Criminal Code of the Federal Democratic Republic of Ethiopia, the 1960 Civil Code, the Computer Crime Proclamation No. 958/2016 and the Freedom of the Mass Media and Access to Information Proclamation No. 590/2008. As a result, the country relies on the existing laws that are found in different pieces of legislation. The country has drafted a comprehensive data protection law, but waits for parliamentary deliberation and approval. Although the right to privacy is enshrined in the Ethiopian constitution, the current laws do not provide full protection to this right, especially in the realm of personal data.

4.6.2 Privacy and Data Protection Laws in Sudan

Content is needed here

4.6.3 Privacy and Data Protection Laws in South Sudan

Content is needed here

4.6.4 Privacy and Data Protection Laws in Somalia

Article 32 of the Federal Republic of Somalia constitution gives the provision of access to information of anyone in the state. The article further continues to state the responsibility of the Federal Parliament in creation of the necessary guidelines to be used, while enacting the provisions stated.

Unfortunately, no guidelines have been developed so far with regards to data protection laws by the parliament.

References

1. The Economist: The World's Most Valuable Resource Is No Longer Oil, But Data, (2017)
2. UNCTAD. (2021). "Data Protection and Privacy Legislation Worldwide | UNCTAD." Retrieved January 24, 2021 (https://unctad.org/page/data-protection-and-privacy-legislation-worldwide).
3. UN. (2015). "Universal Declaration of Human Rights." Retrieved January 24, 2021 (https://www.un.org/en/universal-declaration-human-rights/).
4. **OECD. 2013.** *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
5. Smith, Erin and Peter Rosenblum, Enforcing the Rules (NRGI 2011), available at: http://www.resourcegovernance.org/publications/enforcing-rules
6. Owino, B. (2020). Harmonising data systems for cash transfer programming in emergencies in Somalia. *Journal of International Humanitarian Action*, *5*(1), 1-16.
7. Federal Government of Somalia (2019) *Somalia Social Protection Policy. Federal Government of Somalia, Ministry of Labour and Social Affairs*, Mogadishu.
8. Majid, N., & Harmer, A. (2016). *Collective Resolution to Enhance Accountability and Transparency in Emergencies, Southern Somalia Report*. Transparency International.