REPUBLIC OF KENYA

MINISTRY OF AGRICULTURE,
LIVESTOCK, FISHERIES AND CO-OPERATIVES

DATA GOVERNANCE FRAMEWORK

For Farmers' Registration Data and Roadmap Towards its Operationalization

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

DIGITAL TRANSFORMATION CENTER KENYA

KENYA VISION 2030

THE BIG 4
EMPOWERING THE NATION

ASTGS 2019 2029
AGRICULTURAL SECTOR TRANSFORMATION AND GROWTH STRATEGY
Towards Sustainable Agricultural Transformation and Food Security In Kenya

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

AFA	Agriculture and Food Authority
AGRA	Alliance for a Green Revolution in Africa
ASTGS	Agricultural Sector Transformation and Growth Strategy
ATO	Agriculture Transformation Office
CEC	Country Executive Committee
CTA	Technical Centre for Agricultural and Rural Cooperation ACP-EU
DL	Desert Locust
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
EAGC	Eastern Africa Grain Council
GDPR	General Data Protection Regulation
GODAN	Global Open Data for Agriculture and Nutrition
GoK	Government of Kenya
ICT	Information and Communication Technology
ID	Identity Document
IT	Information Technology
JASSCOM	Joint Agricultural Sector Steering Committee
KAINet	Kenya Agriculture Information Network
KALRO	Kenyan Agriculture and Livestock Research Organisation
KCEP-CRAL	Kenya Cereal Enhancement Programme Program-Climate Resillient Agricultural Livelihoods

KCSAP	Kenya Climate Smart Agriculture Project
KENAFF	Kenya National Farmers' Federation
KNBS	Kenya National Bureau of Statistics
KEPHIS	Kenya Plant Health Inspectorate Services
LDRI	Local Development Research Institute
MoALFC	Ministry of Agriculture, Livestock, Fisheries and Cooperatives
MoICT	Ministry of Information, Communications and Technology
NARIGP	National Agricultural and Rural Inclusive Growth Project
ODPC	Office of the Data Protection Commissioner
RCMRD	Regional Centre of Mapping of Resources for Development
SSF	Small-Scale Farmers
USSD	Unstructured Supplementary Service Data
USAID	US United States Agency for International Development

FOREWARD

In pursuit of 100% food and nutrition security, and in line with the Presidential Big 4 Agenda the Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC) in Kenya developed the 10-year Agriculture Sector Transformation and Growth Strategy (ASTGS 2019-2029). The goal of the ASTGS is to create a vibrant, commercial, and modern agricultural sector that supports 100% food security in the context of devolution anchored on increased producer incomes, increasing agricultural output and value addition, and boosting household food resilience.

The MoAFLC's Digital Transformation roadmap for Kenya's Agriculture sector is important in supporting the ASTGS, and is anchored in the Flagship 8, which seeks to Strengthen research & innovation and enable the launching of priority digital use cases for better decision making and performance management.

Data and digital innovations have been earmarked by the Ministry leadership as key enablers in achieving our ASTGS objectives, with the ministry working to ensure that efforts are streamlined towards Establishment of standards and protocols for a shared data platform to facilitate more evidence-based decisioning and interventions across the sector, while scaling up digital platforms in the agriculture sector.

It is inherent that stakeholders handling farmer and agriculture related datasets work within the required regulatory framework that ensures data security, confidentiality and in conformity with Global Data Protection Regulations (GDPR).

In Kenya, the Office of the Data Protection commission (ODPC) has been the body mandated with Overseeing the implementation of and being responsible for the enforcement of the Data Protection Act (2019). The act has made the provisions for the processing of personal data, rights of data subjects (farmers) and the obligations of data controllers and processors. The ODPC has further outlined the need for data protection impact assessment and ensuring that there are processes in place for organizations to comply with the Data Protection Act.

As a ministry, we have taken concrete steps to ensure our compliance with the Data Protection Act by the development of this Data Governance Framework in consultation with key stakeholders including the ODPC. We are proud to have been the first ministry to host the ODPC in an online session held in November 2021 as we sought to get a detailed understanding of the Data Protection Act and offer guidelines on its compliance.

Consequently, the development of this Data Governance Framework has followed the guidelines provided for in the Data Protection Act and has involved multiple stakeholder workshops, interviews and inputs from across the Agriculture sector.

In order to have the establish the standards and protocols for data sharing across the agriculture landscape, the data governance framework sets the tone for guiding principles and policies for data collection, handling, processing and sharing amongst stakeholders while ensuring personal farmer data is secure and kept confidential.

As we launch this Data Governance framework, it is my hope that we rapidly adopt the defined implementation roadmap in order to enable the processes and systems for seamless exchange of data to further accelerate innovation for our farmers.

This Data governance framework seeks to empower stakeholders with tools and processes to deliver digital innovations targeting over 1.4 million farmers, including the implementation initial use case of farmer registry which is key to providing credible data for providing farmers with e-incentives and e-subsidy which has already been successfully piloted.

To ensure the implementation of this Data Governance Framework, the Agriculture Transformation Office (ATO) while working with key stakeholders in the Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MOALF&C) and through the Digital Transformation Committee (DTC), in close consultation with the county governments should work towards establishing a clear roadmap.

I therefore call upon all stakeholders in the sector to collaborate, align and implement the recommendations of this key Data Governance Framework to enable realization of a thriving digital economy for the Kenyan farmers.

Hon. Peter Munya, EGH
Cabinet Secretary
Ministry of Agriculture, Livestock, Fisheries and Cooperatives

ACKNOWLEDGEMENT

The journey towards development of this Data Governance Framework has involved many stakeholders under the coordination of the Agriculture Transformation Office (ATO).

The support and goodwill from the Cabinet Secretary Ministry of Agriculture, Livestock, Fisheries and Cooperatives, Permanent secretaries and top ministry officials has been pivotal towards this accomplishment. The guidance and advise provided by the Office of the Data Protection Commission (ODPC) has been key in the development of this framework, which is a key milestone for this Ministry.

We wish to thank the public and private sector players who have been instrumental in giving their inputs through participation in workshops and responses through online interviews which took a lot of time and professional commitment. We appreciate the multi-disciplinary team of individuals drawn from both State and non-state organizations who provided their critical insights and reviews for the preparation of this final draft document.

While it is not feasible to list all by name, it is our considered view that every institution whose perspectives, expertise and time went into the just concluded exercise and the ultimate development of this framework deserves a special mention. The invaluable contributions provided by the County Government representatives, farmer organizations, parastatal bodies and our development partners during the consultative stakeholder workshops is highly appreciated.

We express our gratitude to our development partners including Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and Tony Blair Institute for Global Change (TBI) for providing resources for the development of this framework, including the technical assistance and facilitation of the necessary workshops. We are cognizant of the commitment of our donor partners to development of our Data, digitization and digital innovation ecosystems and their key interest in continuously supporting the realization of our ASTGS Flagship initiatives. We look forward to further support for the adoption and implementation of this Data Governance Framework across our ministry as we set the pace for other Government ministries.

Dr. Francis O. Owino, CBS
Principal Secretary
State Department for Fisheries, Aquaculture, and the Blue Economy

Mr. Harry K. Kimtai, CBS
Principal Secretary
State Department for Livestock

Mr. Ali N. Ismail, CBS
Principal Secretary
State Department for Co-operatives

EXECUTIVE SUMMARY

Kenya's Agricultural Sector Transformation and Growth Strategy (ASTGS) seeks to create a vibrant, commercial, and modern agricultural sector that supports 100% food security in the context of devolution. Data and digital technologies take an important enabling role in this transformation and support the sector in reaching its primary objectives to (1) increase small-scale farmer (SSF), pastoralist, and fisherfolk incomes for ~3.3M households and impact ~15M Kenyans; (2) increase food availability year-round by unlocking >500,000 acres of agricultural production and agro-processing across priority value chains; (3) boost household food resilience and reduce the number of food-insecure Kenyans to zero.

The rise of digital and data-driven solutions in agriculture holds the promise of significantly improving agricultural income and livelihoods by giving farmers the tools to boost productivity and profitability. To date, however, low awareness about the benefits of data, as well as the lack of sound data management practices, have affected the trust that farmers have in digital technologies. Consequently, the adoption of digital tools and solutions in the agriculture sector has been slow and wanting. The lack of proper data governance has also led to farmers' data being fragmented and handled by different stakeholders from both the public and private sectors without clear guidance. This has left the farmers with little say in how their data is being used, thus impeding the digital transformation of the whole sector.

To strengthen farmers' trust and give them greater control over who uses the data that is produced on their farms and for what purposes, t*he Ministry of Agriculture, Livestock, Fisheries, and Cooperatives (MoALFC), in its Digitization and Coordination of Kenya's Agricultural Sector Data* guidance document, calls for the development of policies, standards, and protocols to govern agricultural data. Such policies, standards, and protocols, which in their sum constitute what is called a Data Governance Framework, help determine how and when decisions must be made about the gathering and use of agriculture data. Well-functioning Data Governance Frameworks usually accomplish several goals: They (i) highlight rules for data use (e.g., who is allowed to collect and share it), (ii) reduce the risks associated with the collection, storage, and use of data, (iii) ensure clarity and consistency with regards to roles and responsibilities, (iv) help comply with privacy and other regulations, (v) increase value creation through data, (vi) improve data-driven decision making, and (vii) strengthen communication between relevant actors.

As a first step towards a holistic framework governing agricultural data in Kenya, the MoALFC has developed a Data Governance Framework for farmers' registration data in accordance with use case 1 of the *Digitization and Coordination of Kenya's Agricultural Sector Data* guidance document. With the aim of supporting the implementation of the ASTGS Flagship 8 on data and innovation, the framework builds upon already existing policies and guidelines in the field –in Kenya and beyond – and encompasses five central governance pillars. The first pillar defines *roles* and assigns *responsibilities* for decision areas to these *roles.* Data stewards, managers and editors, data handlers, and data experts are the backbone of every Data Governance Framework. The right attribution of these functions and mandates ensures that farmers' data is accurately collected and handled. The second pillar addresses the *regulatory environment for collecting and processing farmers' data* which is largely governed by the Data Protection Act adopted in 2019. Six key data privacy standards such as informed consent and privacy-by-design are outlined, and their applications discussed. The third pillar focuses on the *policies* and *guidelines* needed to set out the context in which the responsible actors and third parties can manage farmers' registration data. Relevant examples hereby include open data and data retention policies or data protection and security guidelines. The fourth pillar of data governance is targeted at *hands-on tools* and *practices* which help individuals and entities apply policies and guidelines. It provides a set of mechanisms and instruments to safeguard the personal data of farmers and facilitate the sharing of agricultural data. The last pillar of the framework tackles questions regarding the *establishment of key processes and procedures for data management* and provides guidance on how to address them.

While the Data Governance Framework developed sets out the necessary parameters to enable sustainable and human-centered data governance in the agricultural sector, it has to be acknowledged that the framework will only deliver on its promises and goals if it translates into action. Hence, it is only to be seen as a stepping stone for the digital transformation aspired to in the ASTGS. However, to help operationalize the Data Governance Framework, a road map with seven key steps to prioritize when working on its implementation has been developed by the MoALFC. The road map is presented in the second part of this document and shall serve as a reference for the next steps to be undertaken. In addition, to help relevant actors in bringing the individual pillars into action, practical templates and examples have been complied in the annexes.

1 INTRODUCTION

The Government of Kenya (GoK) has formulated the Agricultural Sector Transformation and Growth Strategy (ASTGS) to create a vibrant, commercial, and modern agricultural sector that supports 100% food security in the context of devolution. Data and digital solutions play an important enabling role in this transformation, helping the sector to achieve its primary objectives, which are to:

1. increase small-scale farmer (SSF), pastoralist, and fisher folk incomes
2. increase the food available year-round by unlocking >500,000 acres of agricultural production and agro-processing across priority value chains
3. boost household food resilience and reduce the number of food-insecure Kenyans to zero

The Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC) supports this strategy by implementing nine flagships. The Agricultural Transformation Office (ATO) is leading the efforts for the implementation of **flagship 8** titled "Research, Innovation and Data," which is designed to "strengthen research and innovation as launch priority digital and data use cases to drive better decision-making and performance management." Accordingly, the MoALFC has identified **seven priority use cases** aligned with the primary ASTGS outcomes in its strategic document "Digitization and Coordination of Kenya's Agricultural Sector Data." They have been selected due to the essential role the MoALFC takes in developing and scaling them.

One of the underlying challenges for all use cases is the need for seamless and lawful exchange of data and finding the delicate balance between protecting the privacy and confidentiality of farmers' personal data and their economic interest in that data while still leveraging its potential for growth and innovation in the sector. Exchanging agricultural data between actors has, however, to date been far from straightforward and easy in the Kenyan agricultural data space: Not only are there data silos, but data collection efforts are often duplicated. Mistrust between relevant stakeholders impedes on collaboration, and there are significant barriers to scaling data-driven approaches.

Accordingly, as one of the recommended solutions outlined by MoALFC's Digitization Strategy in the form of **use case 7,** standards and protocols – or what could be called a data governance framework – for a shared national agriculture data platform should be established. The data governance framework is hereby set out to cover data access, security, sharing, and ownership aspects of the data collected and processed in use cases 1-6.

Regarding the national agriculture data platform, the Kenyan Agriculture and Livestock Research Organization (KALRO) has been envisioned as its host, given its existing IT capabilities and infrastructure. The platform shall enable more evidence-based interventions from stakeholders with access to it. More specifically, users with access to the platform shall be able to create new knowledge and insights for their interventions from massive volumes of interoperable data that they would not otherwise be able to access cost-effectively

Benefits of the Kenya United Agriculture Data Platform (KUADP strived for, thus include:

- → Enable the Integration of currently siloed digital systems into a unified platform for seamless quality data exchange while also ensuring a robust, secure, and scalable hosting infrastructure connecting to different sources.
- → Facilitate the development of a fully interoperable agriculture data hub ecosystem that includes a national farmer register with a "single-source-of-truth."
- → Ensure Kenya's growth in food production and food security, as Big Data has the potential to unlock complex advanced analytics for future Technology, including machine learning, Artificial intelligence, and other Technology innovations deployments for farmers
- → Linking private sector organizations, development partners, and big Tech-companies with local academic institutions for a conducive research and development environment and further position the MoALFC at the center of critical research collaboration across the Agricultural sector and a champion of Global Open Data policy growth.
- → Attract young talent across the ecosystem, including data scientists, engineers, and architects, to build up and broaden the capability beyond agricultural statistics to further accelerate youth job creation and employment opportunities.
- → Create potential to build clear feedback mechanisms into each proposed intervention & use cases that improve adoption and usability of the solutions with Monitoring and Evaluation of success factors.

2

BACKGROUND

A **data governance framework** was developed for use case 1 to support the implementation of flagship 8 and the digital use cases of the MoALFC Digitization Strategy. Narrowing down the scope of use case 7 to the governance of data for one specific use case hereby offered the opportunity to not only gather learning and best practices along the way but also to develop the first blueprint of a data governance framework with the potential to be applied to the other five remaining digital use cases of flagship 8 in the future.

The Flagship 8 digital **use case 1** aims to accelerate farmer registration and target eligible farmers with e-incentives. It also foresees to rely on performance data analytics to improve the incentive scheme. Hereby it seeks to use digital tools (e.g., e-voucher) to identify the right farmers and to distribute and monitor the performance of the national e-incentive scheme proposed in ASTGS. The digital tools shall increase the likelihood that nationally issued farmer subsidies reach the farmers most in need by eliminating arbitrage opportunities in the current system, including through a digital farmer register managed by the Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC).

The data governance framework presented in the following sections shall therefore be seen as a pilot for the drafting of standards and protocols on data access, security, sharing, and ownership outlined in use case 7 and its key findings and structure as a steppingstone for the development of similar frameworks of the use cases 2-6.

In addition, a **road map towards the framework's operationalization** has also been developed to support the implementation of the designed data governance framework for farmer registration data. The road map encompasses ten key steps which will allow relevant stakeholders to make the data governance framework actionable. It also provides concrete recommendations on how to operationalize the different elements of the data governance framework and what should be prioritized.

3

OBJECTIVE AND METHODOLOGY

The objective for the design of the data governance framework and the roadmap is to:

1 create a common baseline for the collection and processing of farmers' data within the Kenyan agricultural ecosystem and help relevant actors address the needs, challenges, and risks related to the use of farmers' data;

2 increase the understanding among relevant stakeholders about current data management practices in the context of farmers registration and how these intertwine with those of other actors in the space; and

3 support the MoALFC, and other relevant stakeholders from the public and private sector, in operationalizing the data governance framework, i.e., setting up the necessary policies, guidelines, processes and tools.

The development of the data governance framework and the road map followed a **consultative and reiterative approach** with interviews conducted with relevant stakeholders during October and November 2021. Moreover, existing documents regarding data policies and processes provided by the consulted actors were reviewed, and by desk research was carried out.

Moreover, to validate the preliminary findings, a multi-stakeholder workshop was organized on the 30th of November 2021 to present the initial draft of the data governance framework and road map and get feedback.

Table 1: List of consulted stakeholdersocesses and tools.

Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC), Agricultural Statistics Unit, ICT Departments	Global Open Data for Agriculture and Nutrition (GODAN)
Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC), Agricultural Transformation Office (ATO)	Local Development Research Institute (LDRI)
Counties, Joint Agricultural Sector Steering Committee (JASSCOM)	Eastern Africa Grain Council (EAGC)
Kenyan Agriculture and Livestock Research Organization (KALRO)	Regional Center for Mapping of Resources for Development (RCMRD)
Kenya National Bureau of Statistics (KNBS)	Open Institute
Office of the Data Protection Commissioner (ODPC)	Farmers organizations and cooperatives

4

CURRENT STATE OF FARMERS' DATA GOVERNANCE

4.1 TYPES OF FARMERS' DATA COLLECTED

In 2017, the Technical Center for Agricultural and Rural Cooperation ACP-EU (CTA), as a partner of the Global Open Data in Nutrition and Agriculture (GODAN), commissioned a study[1] to compile and categorize the **different types of farmers' data** which can potentially be collected. In 2018, the US Agency for International Development (USAID), in its report on Digital Farmers Profiles[2], complemented the work of CTA with additional data types. Taken together, both studies as well as the consultations with the above-mentioned stakeholders, below is a comprehensive overview of the different types of data falling under the category of "farmers' data":

[1] Boyera, Addison, & Msengezi, 2017

[2] Digital Farmers Profiles: Reimagining Smallholder Agriculture. US-AID, 2018.

Table 2: Farmers' profile data types

DATA CATEGORIES	DATA TYPES
Personal information	» First and last name » ID number » Male/female » Poverty level » Food security level » Marital status (married, single, divorced, widowed, separated) » Family size » Decision-making role on the farm (plot owner, plot manager, labor/support) and in the household
Communication	» Language preference » Phone number » Type of phone » Type of information farmer prefers to receive (on crops, market, etc.) » Mobile phone usage data
Location	» GPS coordinates of the home » Physical address: village, street, number
Farm details	» Land/farm registration number » Labor force/employees (# of people working/ paid to work on the farm) » Equipment owned (planting, harvest, post-harvest equipment) » Livestock (types and numbers) » Farm geo-shape/polygon*

DATA CATEGORIES	DATA TYPES
Field information	» Location of plots » GPS of plots » GPS accuracy*, i.e., 4 meters » Geo-mapping/geo-fencing » Size of field » Elevation » Soil conditions » Land title » Crop history (crops grown over time) » Type of watering/irrigation sources
Value chain information	» Crops grown » Varieties grown » Seed types and amount used » Spacing of plants » Equipment used
Production information	» Date of planting » Spacing of plants » Intercropping » Weather data (rainfall, temperature, hygrometry) » Yields (date of harvest, etc.) » Pest/disease attacks » Post-harvest (storage, sales) » Adherence to Good Agricultural Practices (GAPs); types of planting, fertilizer, pest control, harvesting techniques used
Financial instruments	» Account ownership (does the farmer have an account?) » Mobile account ownership » Remittances » Payments/cash transfers » Financial services providers who hold/ facilitate farmers' transactions

DATA CATEGORIES	DATA TYPES
Credit	» Whether credit accessed, loan size, use of loan » Farm business plan details
Insurance	» Fields (livestock) covered » Risks covered (and period) » Insurance company name » Cost » Amount repaid if one of the risks covered happens
Qualifications / Certifications	» Training attended » Certifications received » Monitoring of compliance to standards
Business information	» Cooperative memberships » Agribusiness linkages » Markets farmers are linked to » Sales prices

** Additional types of data added and not yet listed in the USAID and CTA studies*

According to the Digitization Strategy of the MoALFC, there are **six types** of farmers' registration data currently collected:

→ Farmer national ID number

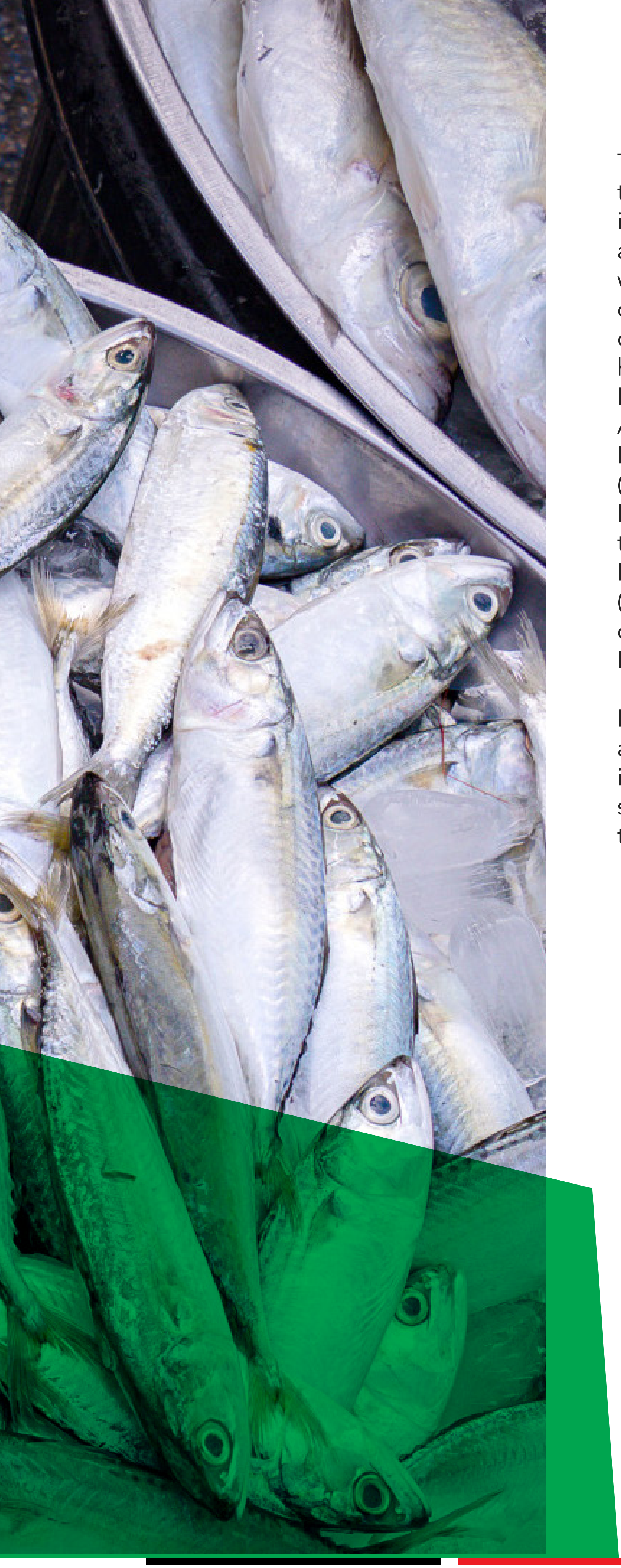
→ Name

→ Mobile number

→ Location

→ Size of land

→ Value chains grown



The stated goal of the data collection is to support farmers in investing in yield improvement (i.e., buy the right inputs at the right time and use them the right way) by providing them with e-vouchers on their mobile phones based on a set of eligibility criteria. The farmer data holders outlined are the Kenya Cereal Enhancement Program-Climate Resilient Agricultural Livelihoods (KCEP-CRAL), Kenya Climate Smart Agriculture Project (KCSAP), National Agricultural and Rural Inclusive Growth Project (NARIGP) (all three development partners), DigiFarm, Kenya National Farmers' Federation (KENAFF) (both private sector initiatives) counties, KALRO as well as Huduma Namba and the population census (GoK).

Beyond that, the use case foresees to also collect additional farmers' data when it comes to impact monitoring of the subsidies issued to the farmers. The data types gathered in this context include:

→ The yield of value chains produced, e.g., kgs/head of cattle, tons of fish landed per species, etc.

→ The yield of value chains produced, e.g., kgs/head of cattle, tons of fish landed per species, etc.

→ Type of inputs (i.e., subsidies) received

→ Price of inputs received

→ The geographic location of inputs received

These data types are collected via Unstructured Supplementary Service Data (USSD) survey and assessed by KALRO with the aim of drafting reports on the impact of the provided inputs for the MoALFC for improvement of the farmer eligibility criteria for inputs. Likewise, non-personally identifiable data shall be made available to the public over the platform. The private sector can also rely on it to better inform production and distribution decisions. In both cases, it is foreseen for the data to the collected/updated every season, i.e., four times a year.

A **challenge in the collection of this data** currently is that while farmers' profile data is available, it is incomplete and fragmented and requires compiling of databases and additional registration of farmers for full coverage. Moreover, as highlighted in the Digitization Strategy, much of the agricultural data is currently being collected and stored by multiple stakeholders such as public sector institutions, private sector players, and development partners. More than seven online government databases exist, to date, for agricultural data, including the Kenya Agricultural Information Network (KAINet). Many of these databases have moreover not been updated in several years. E.g., there are profiles of ca. two million farmers registered on three platforms, i.e., DigiFarm, MOA-Info, and One Acre, as well as 540.000 registered farmers at KALRO.

Another challenge emerging from the desk research, interviews and consultations conducted is that the **opinions and practices vary** when it comes to the interpretation of the types of farmers' data to be collected. Also, no common understanding exists among relevant stakeholders regarding the purpose for which the farmers' data is to be collected. While the specific reasons for data collection appear to be different from actor to actor, the overall common objectives can broadly be defined as understanding farmer needs for products, information services, market linkages, and finance.

4.2 REGULATORY ENVIRONMENT WITH REGARDS TO PERSONAL DATA

While agricultural data is not generally considered as 'personal data,' there are certain data types like name or mobile number that are clearly personal. There are, however, also certain data types that do not appear to be personal at first sight but, under some circumstances, can identify a farmer and thus become personal information. An example of such personal data is GIS or location data. If the geographic coordinates are known and combined with other data points, the data may then point to a specific farmer. This GIS location data would then have to be considered personal data.

DEFINITION OF PERSONAL DATA

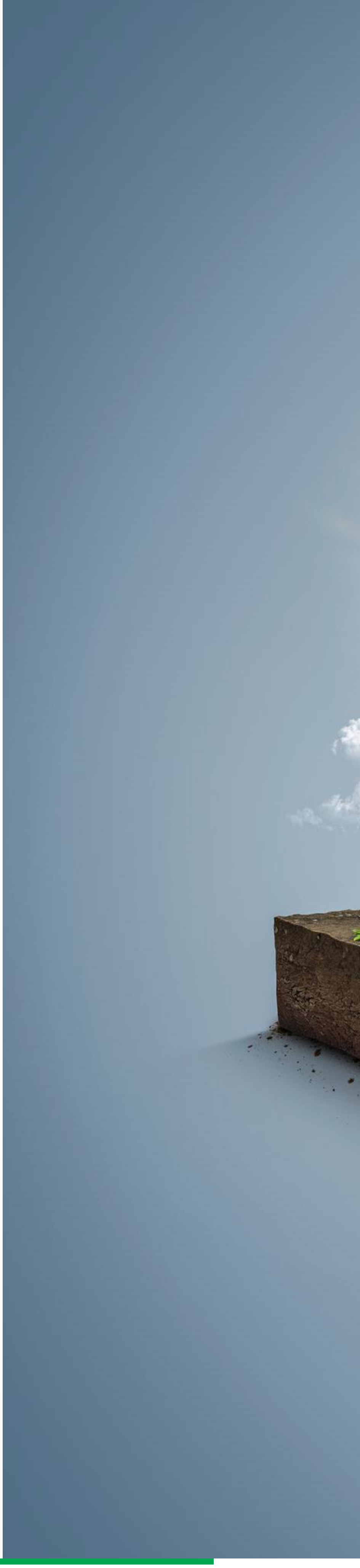
Under the Data Protection Act, personal data refers to any information relating to an identified or identifiable natural person. An identifiable natural person means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, and an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity.

The most important legislative document governing the usage of farmers' data in Kenya is the **Data Protection Act (DPA)** which was passed in November 2019 to regulate the processing of personal data and the protection of data subjects' privacy rights.

The DPA stresses that every data controller or processor (i.e., agro-dealers, government agencies like the MoALFC, and any other actors collecting and processing farmers' data) must ensure:

- Adherence to the right of the data subject to privacy.
- Lawfulness, fairness, and transparency.
- Purpose limitation, i.e., processing personal data for explicit, specified, and legitimate purposes.
- Principle of data minimization, i.e., personal data should be adequate, relevant, and limited to what is necessary for data processing purposes.
- Provide the data subject with valid explanation whenever information relating to family or private affairs is required.
- Accuracy. Personal data should be up to date and reasonable steps should be taken to ensure that any inaccuracy is erased or rectified without delay.
- Storage limitation, i.e., personal data should not be kept for periods longer than the purposes it was collected for.
- Personal data is not transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

These principles have become known as the **Data Protection Principles** (section 25 of the DPA). The passing of the DPA came in the context of implementing the General Data Protection Regulation (GDPR) of the European Union in May 2018.



DEFINITION OF NON-PERSONAL DATA

Non-personal data is data or information that cannot be used to identify a person. Often, data such as agronomic data (e.g., yield, nutrient, soil), machine data (e.g., fuel consumption, engine performance), and weather data is non-personal data and therefore is not governed by the DPA.

The **objectives** of the DPA can be summarized in five main points:

- Give effect to Article 31(c) and (d) of the Constitution that contains the right to privacy
- Establish the Office of the Data Protection Commissioner (ODPC) as enforcement body for the law
- Regulate the processing of personal data
- Provide for the rights of data subjects
- Set out obligations of data controllers and processors

Looking at the **regulated actions covered** by the DPA, the following can be outlined:

- Data collection.
- Type of data to be collected.
- Security of collected data.
- Disclosure of data.
- Retention of data.
- Accuracy of the data.
- Deletion of data; and
- Updating of data.

better articulate the benefits of doing business
6
7
8
18,321
Registered Users
Realtime Dashboard
37.91%
31.86%
30.23%
Focus on Your Finances
Whether you're a full time, part time or freelance photographer - or even if you make a few bucks on the side from your photography - you are your own business.
Target

Given that some of the farmers' data sets collected in use case 1 fall under the definition of personal data, their usage has to be compliant with the DPA. There are **eight legal bases for the lawful use of personal (farmers) data** that data processors and controllers in the agriculture sector have to consider. Personal farmers' data can be processed if:

- → The data subject (farmer) consents
- → For contractual purposes
- → To be compliant with a legal obligation
- → For legitimate interests
- → For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- → For the performance of any task carried out by a public authority
- → For the exercise, by any person in the public interest, of any other functions of a public nature; to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
- → For historical, statistical, journalistic, literature and art or scientific research.

For the data types under use case 1, which are non-personal data, the Data Protection Act does not apply. For these types of data, no public legislative framework governing their use exists. Their transaction is currently governed by contracts and licensing agreements. However, the terms of these contracts and agreements are often complex, which leaves smallholder farmers with very little negotiating power and mistrustful.

Finally, another important element in the collection and processing of personal data under the DPA is asking the question of who the data controllers are and who are the data processors of farmers' data. The law recognizes that not all organizations involved in processing personal data have an equal level of responsibility. The definitions of controllers and processors can be articulated as follows:

DEFINITION OF A DATA CONTROLLER

A data controller is a natural or legal person, public authority, agency, or other body that alone, or jointly with others, determines the purpose and means of processing personal data.

DEFINITION A DATA PROCESSOR

A data processor is a natural or legal person, public authority, agency, or other body, that alone or jointly with others processes personal data on behalf of the data controller.

If an agriculture stakeholder is classified as a data controller or a data processor, it is responsible for ensuring that it complies first with the data protection law and demonstrates compliance with the regulation's data protection principles. It ensures privacy by design and default by taking all the necessary technical measures and safeguarding data subjects' rights.

It is worth noting that these basic obligations apply to both the data controllers and the data processors. Furthermore, according to section 18 of the DPA 2019, all data controllers and data processors are required to be registered with the Commissioner. The Commissioner is required to prescribe thresholds for mandatory registration and to consider the nature of the industry, the volumes of data processed, whether sensitive personal data is being processed, amongst other matters. The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.

The data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller. As it has already been noted, the data controllers and data processors have the same basic obligations, but they do not have an equal level of responsibility. Below is a more precise explanation of data controllers' and data processors' obligations.

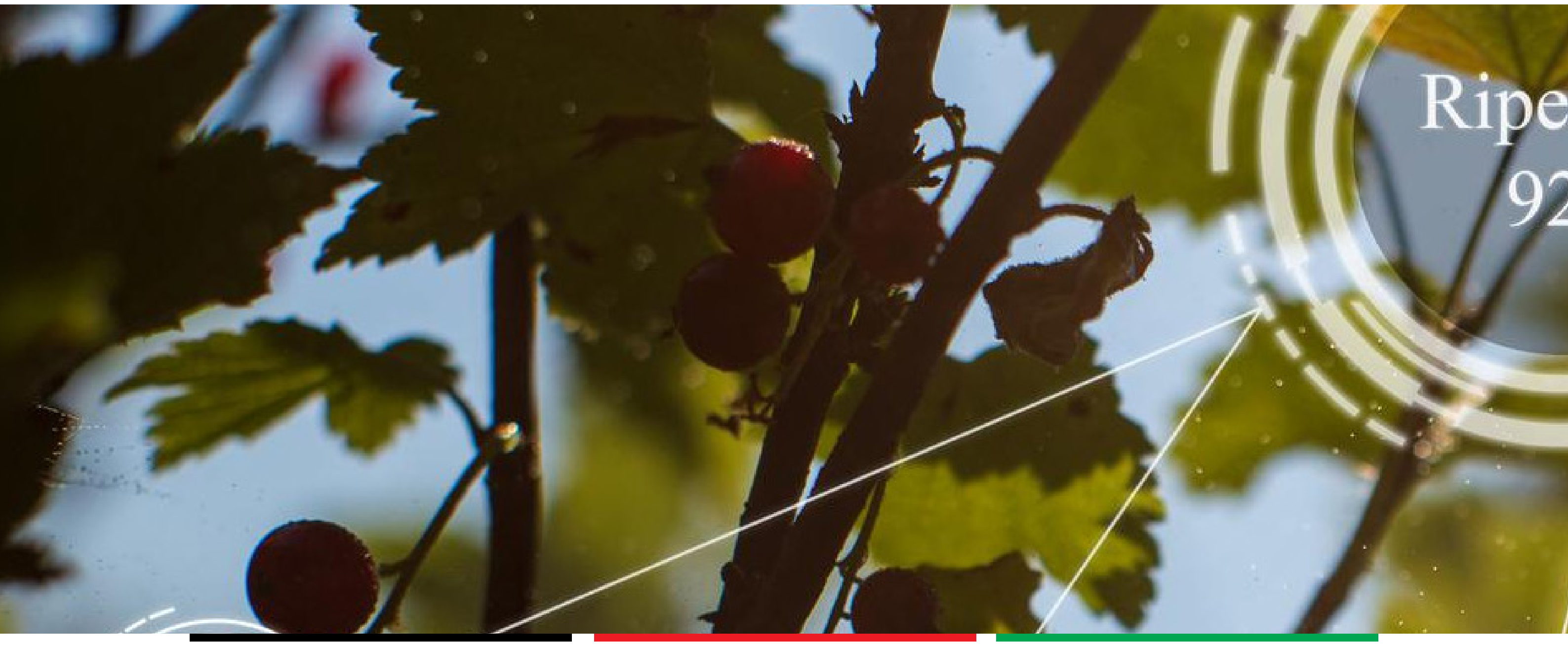
Obligations of a data controller under DPA 2019

→ The data controller must exercise overall control over the purpose for which, and the way, personal data is processed. Therefore, activities such as interpretation, the exercise of professional judgment, or significant decision-making in relation to personal data are a data controller's responsibility.

→ The data controller is responsible and must demonstrate compliance with the eight above aforementioned principles relating to the processing of personal data (duty of accountability).

→ The data controller is also responsible for the compliance of their data processor(s).

→ The data controller is legally responsible for the processing of personal data and is liable for any damage caused by the processing and in case of a data breach.



Obligations of data processors under DPA 2019:

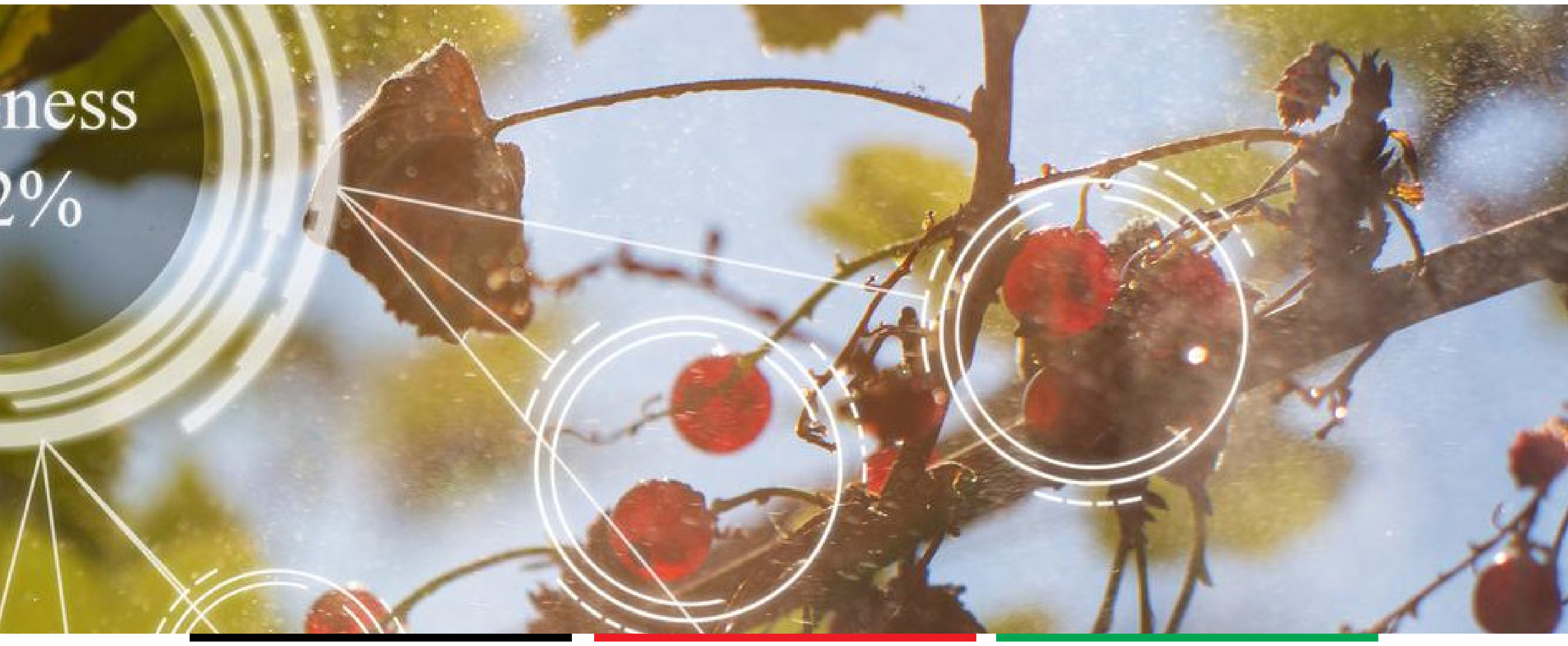
→ The data processor's main responsibility is to process the personal data it receives strictly based on the instructions of the data controller. The data processor will also need to take all the proper measures to protect and safeguard personal data to ensure data security, including protection against accidental or unlawful destruction or loss, alteration, unauthorized disclosure, or access.

→ The data processor should demonstrate compliance with the eight principles relating to the processing of personal data.

→ The data processor cannot bring in another processor without authorization from (and thus notification duty towards) the controller. In addition, a data processor who, without lawful excuse, discloses personal data processed by the data processor without the prior authority of the data controller commits an offense.

→ A data processor involved in the processing of personal data is liable for damage caused by the processing only if the processor — (i) has not complied with an obligation under the Act specifically directed at data processors; or (ii) has acted outside, or contrary to, the data controller's lawful instructions.

→ Notification of personal data breaches. If a data processor becomes aware of a personal data breach, they must notify the relevant controller without undue delay. A data processor must also assist the data controller in complying with its obligations regarding personal data breaches.



4.3 ALREADY EXISTING POLICIES AND GUIDELINES ON FARMERS' DATA

In the agricultural sector in Kenya, some policies and guidelines have already been developed by various stakeholders in relation to farmers' data. In the following, a short overview of the most important and relevant ones is provided, which could be used as a good starting point for the development of data policies for the Kenya United Agriculture Data Platform (KUADP.

KALRO is keeping a farmer register that collects farm data that, among others, includes personal data such as biographical data, demographic data, location, farm area geo-recording, and data value chains. Since there are concerns around data collection and sharing, such as data misuse, privacy violations, security issues, data inaccuracies, conflict of interests, and lack of digital literacy with regards to the data in question, KALRO has developed the following policies: KALRO research data policy: It aims to ensure that all relevant data is collected, appropriately managed, and made available to the public and all partners and stakeholders. This policy explicitly guides the organization in managing and using data around the following 6 topic areas:

1 Collection of research data

2 Retention of research data

3 Access to research data

4 Data from collaborative research

5 Collection and handling of restricted data

6 Dissemination and publication of data products and services

The policy also provides guidelines around the collection of farmers' data, ownership issues and intellectual property (IP) rights.

KALRO ICT policy: The broad objective of KALRO is to develop a knowledge management platform that will enhance knowledge sharing and dissemination across the organization and key stakeholders. Therefore, the ICT policy objective is the implementation of infrastructure for enhanced security and integrity as well as reduced redundancy of ICTs. It entails sub-policies that cover the following topics:

ICT infrastructure development

1 Adoption of Standards for ICT governance

2 Establishment of ICT Units

3 Information Security Management System

4 Access to ICT infrastructure and information

5	Protection of intellectual property
6	Monitoring the use of ICT
7	Safe and Appropriate Use of ICT Hardware

Users' security access control policy: It provides the guiding principles through which users can ensure proper access control of ICTs accessible to them. The purpose of this policy is to protect KALRO in the eventuality of a systems breach. In addition, the policy is intended to safeguard the organization, users, and owners of IP rights from access control security-related incidents and any consequential action, e.g., loss of information. Among others, the policy sets data protection principles and defines users' responsibility for electronic security access and control (e.g., password requirements).

Both the KALRO data research policy and the ICT policy should be examined in conjunction with the KALRO data management policy.

KALRO ICT open data policy and strategy – Towards food security in Kenya: This policy aims to foster an enabling environment that will regulate the everyday operations of publishing data and also ensure the reusability of the data. It addresses and outlines:

- → Open data concepts and principles
- → Data set formats and standards
- → The interaction between data providers and data users
- → The supply and demand chain of published data sets
- → Quality control measures for the data sets
- → Mechanisms to update the data regularly
- → Initiatives and incentives for stakeholder participation in open data

Beyond the policies developed by KALRO, the following policies and guidelines are relevant:

The Draft Agriculture Policy (Feb 2019) to be signed: The policy outlines policy statements and articulates the position of national and county governments on issues important to the use cases – including information and data management, extension, research and development, and human resource development.

Agricultural and Nutrition Data Collection and Management (ADCM) Guidelines: They have been developed by the State Department for Crop Development and Agricultural Research of Agriculture of the MoALFC to enable officials and other stakeholders at various levels to adopt a common approach to agricultural and nutrition data collection and management based on universally recommended procedures. The Guidelines are also intended to improve the availability, quality, and reliability of agricultural and nutrition data through enhanced data validation, analysis, dissemination, archiving, and use of modern technology. The Guidelines are organized in the form of sub-themes for each chapter. For every sub-theme, the adopted organization includes an introduction with basic principles for the sub-theme, type of data to be collected, requirements for data collection, and procedures for data collection. Also

included for each sub-theme are the reporting tables and reporting formats at various levels of data reporting. For practical application, these Guidelines are to be used together with the *Agricultural and nutrition data Collection and Management Training Manual,* which the State Department of Agriculture has developed.

The Regional Centre for Mapping of Resources for Development (RCMRD) Data Management Policy: The objective of this policy is to set standard principles around data management in order to maintain the value and ensure the effective use of data within the organization. It is recommended as a good reference point for the development of relevant policies about farmers registration as it defines in a very concrete way possible roles and responsibilities among the actors, decisions about data access, data collection and maintenance, data documentation, a data inventory system, data quality, data ownership, and data security issues.

5

STAKEHOLDER MAPPING

A key element of data governance is collaboration. The governance of data requires a transformative and cultural change process that relies largely on the collaborative efforts of the stakeholders to be successful. It is therefore essential to identify relevant stakeholders within a given data space, in this case, farmer registration data, and to gain a better understanding of their (possible) roles in the governance of the data in question.

Table 3: Stakeholder Map Farmers' Registration Data Space

NAME	DESCRIPTION
Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC), Agricultural Statistics Unit	The MoALFC is the data controller for the Kenya United Agriculture Data Platform (KUADP. It will define the purpose and the means for farmers' registration as already mentioned in use case 1. Overall, the MoALFC will manage the digital farmers' register. It will collaborate with various stakeholders (public institutions, private sectors) by signing data sharing agreements (e.g., defining data ownership) and determining the roles and responsibilities of each actor in the development of the data governance framework. In addition, the MoALFC will appoint representatives as members of the Data Governance Council.
Ministry of Agriculture, Livestock, Fisheries and Cooperatives (MoALFC), Agricultural Transformation Office (ATO)	ATO is a multidisciplinary unit established by the MoALFC. It is the delivery mechanism for the identified use cases in the Digitization Strategy of the Ministry. More specifically, it will facilitate the coordination of use case 1 in conjunction with use case 7 and could act as a Steering Body for the implementation of the data governance framework.
Ministry of Information, Communication and Technology (MoICT)	The MoICT will provide guidance to MoALFC, KNBS, and KARLO about the standards and guidelines for technical infrastructure, data interoperability, regulation on privacy and security, and systems integrity which are necessary for developing use case 1.
Counties, Joint Agricultural Sector Steering Committee (JASSCOM)	County Governments are responsible in the area of agriculture, among others, for crop and animal husbandry, livestock sale yards, county abattoirs (slaughterhouses), plant and animal disease control, and fisheries. The Counties are responsible for farmers' data collection and sharing via their databases to avoid any duplication for farmers' registration. JASSCOM will assist and oversee the Counties with the implementation of the data governance framework.

NAME	DESCRIPTION
Council of Governors (COG)	The COG was established under the Intergovernmental Relations Act. This is a body consisting of the elected governors of the 47 counties. It will provide consultation among county governments, in the execution of their functions in relation to farmers' registration (collection, use and sharing of farmers' data). The county-level delivery functions should be embedded within existing structures in the COG, JASCCM, and county-level leadership, with the COG encouraged to domesticate ATO activities at the county level within the County Agricultural Committees as necessary.
Kenyan Agriculture and Livestock Research Organization (KALRO)	KALRO is a national organization created under the Kenyan Agricultural and Livestock Research Act 2013, to establish a suitable legal and institutional framework for coordination of agricultural research in Kenya. One of its goals is to expedite equitable access to research information, resources, and technology, promote data sharing and improve capacity and practices. It will be the host of the Kenya United Agriculture Data Platform (KUADP for use case 1 as it provides the necessary IT infrastructure and already has experience in managing farmers' profiles (farmer registers) and developing policies (e.g., research data policy, ICT policy, data management policy) which address issues around data ownership, data protection, and security.
Kenya National Bureau of Statistics (KNBS)	The government institution is responsible for the enforcement and implementation of the Data Protection Act 2019. ODPC will provide relevant guidelines on farmers' consent, data rights, DPIAs, etc.

NAME	DESCRIPTION
Global Open Data for Agriculture and Nutrition (GODAN)	GODAN is an international alliance that aims to promote the global availability of open data in agriculture. Its focus is on building high-level policies, raising awareness and collecting best practices. It can contribute to the development of an open data policy in the context of the data governance framework.
Local Development Research Institute (LDRI)	A non-profit organization that could provide technical assistance to the MoALFC to help implement and support evidence-based improvements to policy and regulatory frameworks as well as performance management in relation to open data.
Eastern Africa Grain Council (EAGC)	A non-profit organization that prepares, disseminates, and promotes the exchange of information on matters affecting the regional grain industry (RATIN System). EAGC keeps a farmer's registration and has developed policies on privacy and confidentiality.
Regional Center for Mapping of Resources for Development (RCMRD)	RCMRD is an inter-governmental organization with 20 contracting Member States in the Eastern and Southern Africa Regions. It promotes sustainable development through generation, application and dissemination of geo-information and ICT services and products. RCMRD is developing a data management policy that could be used a good reference point for implementing the data governance framework.

NAME	DESCRIPTION
Open Institute	A non-profit organization that collaborates with Governments, civil society, citizen groups, and private sector companies to make information available to the public, taking into consideration the privacy and data protection rights of the individuals. The Open Institute can support the MoALFC in deciding which data will be open, which will be considered public data and what restrictions might be relevant to privacy and data security. Recently it released a report on data protection and access to information in Kenya in relation to the Data Protection Act 2019 (available here: https://restoredatarights.africa/resources/a-study-on-national-and-sub-national-data-practices-in-kenya/).
Alliance for a Green Evolution in Africa (AGRA)	AGRA aims to transform the agricultural system and increase the productivity and income of smallholder farmers by advocating for policies, capacity building, and promoting partnerships with the private sector.
National Cereals and Produce Board	This is a state corporation with a Statutory Board under the MoALFC. Its trading division operates an agricultural hub model that involves the registration of stakeholders such as farmers.
Kenya National Federation of Farmers (KENAFF)	KNEAFF is a non-political federation of all Kenyan farmers (farmers' organization). It represents the Kenyan agricultural sector within the Kenya Private Sector Alliance (KEPSA) as the board chair. It could collaborate with the MoALFC and the Counties to ensure effective representation of farmers in respect to their personal data and rights in the context of the implementation of the data governance framework.

NAME	DESCRIPTION
Agriculture and Food Authority (AFA)	The role of AFA is to regulate, develop and promote scheduled crops value chains for increased economic growth in Kenya. It is a state corporation under the MoALFC. In consultation with the county governments, some of its functions are to regulate and promote best practices, collect and collate data, maintain a database on agricultural products excluding livestock products, document and monitor agriculture through registration of farmers as provided for in the Crops Act.
County Executive Committee (CEC) Caucus	The County Executive Committee implements and coordinates development projects of the Counties. The committee also implements the laws the County Assembly passes and ensures compliance by the various county departments. The county executive committee is tasked with managing, coordinating, and implementing County Government plans and policies.
Kenya Plant Health Inspectorate Services (KEPHIS)	KEPHIS is a government organization whose responsibility is to assure the quality of agricultural inputs and produce to prevent adverse impacts on the economy, the environment, and human health. There is a farmers' registration database available, and policies have been developed on data management.
Farmers' organizations and cooperatives	They can play a significant role as farmers' data stewards. They could play a leading role in the creation, negotiation and adoption of a Code of Conduct on behalf of their farmers.
Konza Technopolis	It is a key flagship project of Kenya´s vision 2030 economic development portfolio. Konza could provide its knowledge and expertise on ICT technology, superior, reliable infrastructure, and business-friendly governance systems, policy, and regulatory frameworks.

The participation of these stakeholders is considered essential in the discussions for the validation and implementation of the data governance framework for farmers' registration data. Many of them have already developed policies, processes, and best practices around farmers' data sharing that can be used as a reference point for the MoALFC and avoid duplications.

6

DATA GOVERNANCE FRAMEWORK FOR FARMERS' REGISTRATION DATA

Farmers' registration data and their use for improved decision-making and innovation are critical aspects for the digital transition of the Kenyan agricultural sector. Unspecified and fragmented data governance modalities have given rise to concerns about how farmers' data is gathered, thus reducing farmers' willingness to adopt digital tools and services. This affects the availability and accessibility of data relevant for the digital use cases 2-6 and therefore impedes the development of the agricultural sector.

Accordingly, the development of clear, transparent, and rights-based governance processes for farmers' data is essential. In the following section, an overview of the data governance framework for farmers' registration data will be presented, and its individual pillars discussed. Considering the facts, the objectives, and the farmers' data types to be collected regarding the impact monitoring of provided subsidies is yet to be further clarified between stakeholders, the framework will **focus on the farmers' registration data and farmers' data related to impact reporting** as mentioned in 4.1. Before taking a deep dive into the various aspects of the framework, it iscritical to create a common understanding of what is meant with the concept of a data governance framework.

Overall, a data governance framework thus provides a framework for the development and enforcement of policies, standards, principles, and guidelines that address issues such as the circumstances under which data can be accessed, privacy and confidentiality of individuals, and compliance with relevant legislation. A well-planned data governance framework ensures that data is trusted, well-documented, and easy to find and that it is kept secure, compliant, and confidential.

6.1 DEFINITION

Definition

Derived from Growing a digital future: Creating a data governance framework (2019), Assoc. Prof. Leanne Wiseman et al.

A data governance framework determines how and when decisions need to be made about the collection and use of data, and provides the framework to facilitate those decisions. A clear set out data governance framework will accomplish many goals, including:

- Provide clarity and consistency on roles and responsibilities
- Establish rules for data use (e.g., collection and sharing)
- Minimize the risks of collecting, storing. and using data
- Help meet regulatory expectations
- Improved decision making
- Improved communication
- Increase the value of data

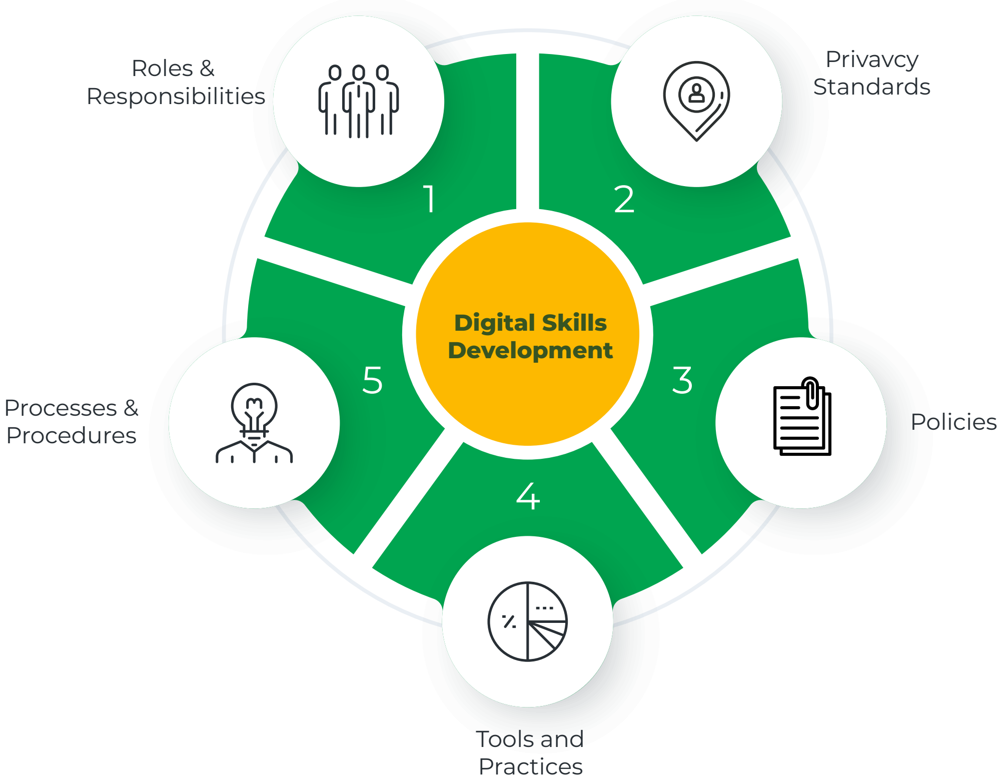
6.2 THE FIVE PILLARS OF DATA GOVERNANCE

Applying the concept of a data governance framework to farmers' registration data, five central pillars can be highlighted, which form the baseline for well-functioning data governance:

The first pillar focuses on roles and responsibilities. Data stewards, data managers and editors, data handlers and data experts are the backbone of every data governance framework. The right attribution of these roles and responsibilities ensures that farmers' data is accurately collected, turned into interoperable quality data sets, uploaded in time onto the Kenya United Agriculture Data Platform (KUADP, and processed and accessed in compliance with relevant privacy and security standards. Investing heavily in the training and education of these key personnel is essential.

The second pillar is the regulatory environment for collecting and processing farmers' data. As elaborated in section 4, ensuring the legal basis for using and sharing farmers' registration data is the foundation to leverage data responsibly and confidently for better decision-making and innovation. However, there are also six additional data privacy standards to ensure that the collection and processing of farmers' registration data is in line with the Data Protection Act, namely, (i) ensuring informed consent, (ii) applying privacy-by-design, (iii) complying with data subjects' rights, (iv) breach notification and (v) the appointment of Data Protection Officers.

Illustration 1: Data Governance Pillars



The third pillar addresses policies and guidelines that set out the context in which the people responsible and third parties manage and use farmers' registration data.The core purpose of policies and guidelines around farmers' data is to recognize that it is a critical asset and must be treated as such. Relevant policies and guidelines that need to be developed under this pillar are (i) an internal data governance policy, (ii) an external (open) data policy, (iii) internal data protection and security guidelines, as well as (iv) a data retention policy.

The fourth pillar of data governance focuses on tools and practices which help responsible individuals and entities apply the policies and guidelines outlined in the third pillar. The first set of tools encompasses instruments to safeguard the personal data of farmers, namely, (a) information on how to anonymize and pseudonymize data, (b) a data protection impact assessment (DPIA), (c) best practices on data minimization, as well as (d) an informed consent template. The second set of instruments centers on facilitating the sharing of farmers' data. To address the challenges of business-to-business (B2B) and business-to-government (B2G) data sharing, an online tool for drafting an agricultural code of conduct is discussed and provided. It helps set common standards for data-sharing and provides principles that the signatories agree to apply in their data sharing contracts. As a complementary instrument, a template and guide for the drafting of data sharing agreements are outlined. Furthermore, to assist actors in keeping an overview of the different types of data collected, used, and shared under use case 1, templates for data inventories as well as a data license register are provided under pillar four.

Finally, the fifth pillar addresses questions regarding the establishment of key processes and procedures for data management in the realm of use case 1 on farmers' registration. Mapping processed data is essential in relation to data flows, actors, and activities, from data collection to data sharing (Standard Operating Procedure format). These processes and standards include definitions of how data will be stored, moved, changed, accessed, and secured. Mechanisms to monitor data quality need to be established as well.

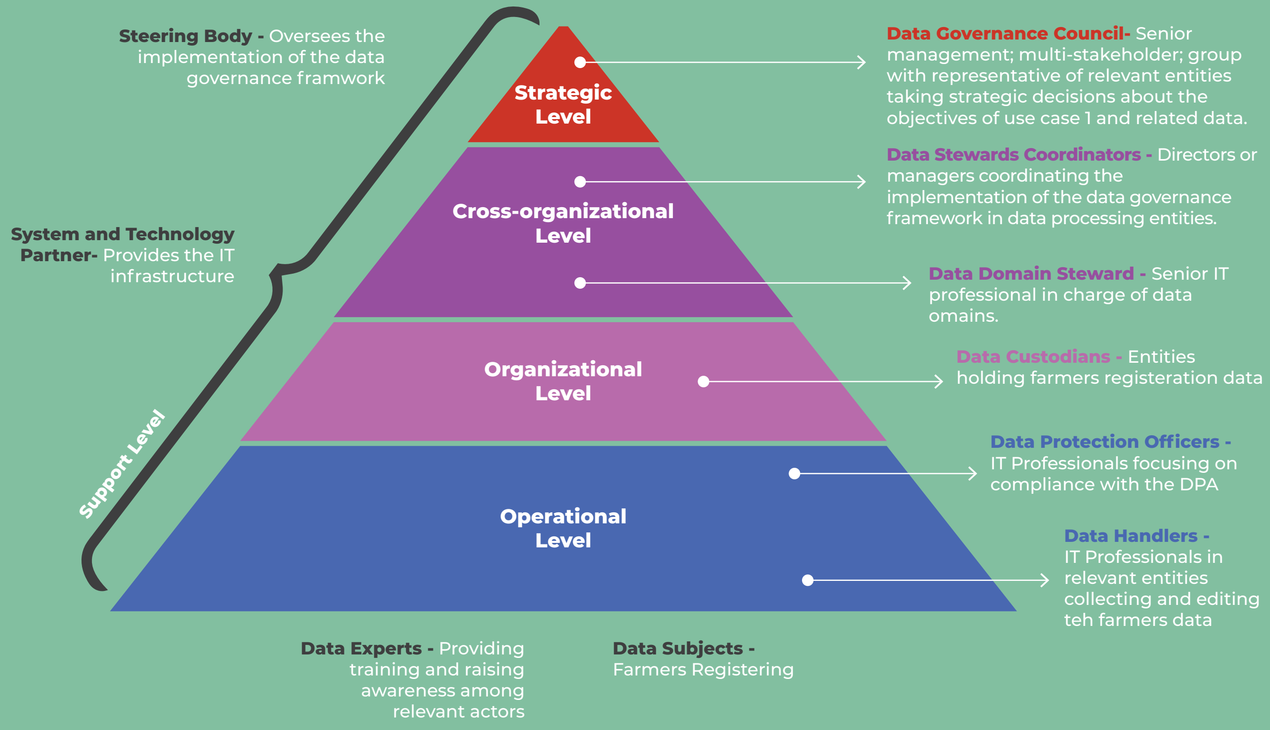
The following table discusses the five data governance pillars in detail. However, before taking a more in-depth look at the individual pillars, it should be noted that the development of data governance frameworks for the agricultural sector is nothing fundamentally new. Over the last year, different organizations and actors have designed and implemented frameworks better to govern their agricultural data within a given data ecosystem. Hence, the different pillars outlined in the subsequent sections have been drafted in the spirit of not reinventing the wheel but building and reusing already existing best practices and examples. Accordingly, throughout the sections of the framework, reference is made to available resources and materials from other contexts.

6.3 DATA GOVERNANCE FRAMEWORK FOR FARMERS REGISTRATION DATA (USE CASE 1 DIGITIZATION STRATEGY MOALFC)

PILLAR 1 (including the cross-cutting topic of digital skills)

Roles and Responsibilities

The different roles and responsibilities suggested as part of the data governance framework for farmers registration data are presented below. This list of roles and responsibilities should be used as a "living" document and adjusted if changes become necessary in the process of implementing the framework.



Steering Body - Oversees the implementation of the data governance framwork

System and Technology Partner- Provides the IT infrastructure

Data Governance Council- Senior management; multi-stakeholder; group with representative of relevant entities taking strategic decisions about the objectives of use case 1 and related data.

Data Stewards Coordinators - Directors or managers coordinating the implementation of the data governance framework in data processing entities.

Data Domain Steward - Senior IT professional in charge of data omains.

Data Custodians - Entities holding farmers registeration data

Data Protection Officers - IT Professionals focusing on compliance with the DPA

Data Handlers - IT Professionals in relevant entities collecting and editing teh farmers data

Data Experts - Providing training and raising awareness among relevant actors

Data Subjects - Farmers Registering

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
Data Governance Council (Strategic level)	» The Data Governance Council is responsible for the strategic guidance with regards to the data governance framework on farmers' data, prioritization of the objectives for the farmers data used, approval of ecosystem-wide data policies and standards for the data in question, as well as enabling support, understanding and awareness about the data governance framework. » The responsibilities of the Data Governance Council include: » Becoming educated in what data governance means, how it can and will work for use case 1 and what it means to embrace data governance and activate relevant stakeholder data stewards. » Approving things that need to be approved – i.e., internal data governance policy, external (open) data policy, data retention guidelines, tools, etc. » Pushing data governance into their organizations by actively promoting improved data governance practices. » Meeting regularly to stay informed of data governance framework implementation for use case 1. » Identifying and approving of pivotal data governance roles including cross-department and organization domain stewards.	Multi-Stakeholder group with representatives of MoALFC, KALRO, KNBS, JASSCOM, GODAN, farmers associations

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
Steering Body (Support level)	» The Steering Body is responsible for overseeing and coordinating the implementation of the data governance framework across departments and organizations. The role of the Steering Body is to serve as the conduit between the different stakeholders and the data governance council and is authorized to make decisions and take actions regarding the framework. Another important role is for it to appoint the data governance lead (i.e., this could be a Chief Data Officer position) and the members of the Data Governance Council. » Overview of responsibilities: » Administering the framework, including facilitating the data governance council meetings » Developing and delivering data governance educational, awareness, and mentoring materials and trainings » Providing quality assurance – oversight, monitor results, report to the Data Governance Council » Establishing, maintaining, and periodically reviewing and recommending changes to data governance policies, standards, guidelines, and procedures when necessary » Supporting data quality issue analysis and solving » Conducting audits to ensure that policies and processes are in place and functional for maintaining and improving the framework » Sponsoring, approving, and championing the data governance framework.	This role could be filled by ATO and the proposed Digital

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
System and Technology Partner (Support level)	The System and Technology Partner is the entity hosting the central database for the farmers registration data collected and to be processed. *Overview of responsibilities:* » Securing IT infrastructure for the Kenya United Agriculture Data Platform (KUADP » Ensuring the security of the platform against cyber threats » Assuring that sensitive data, regardless of format, is protected at all times by only using approved equipment, networks, and other controls.	KALRO and other Government ICT
Data Steward Coordinators (Cross-organizational level)	» Data stewards are the individuals in relevant organizations responsible for overseeing farmers' registration data and implementing related policies and processes, e.g., compliance with data protection standards. » Overview of responsibilities: » Identifying and documenting regulatory and legal/risk issues » Ensuring that the policies, procedures and tools are in place for maintaining / improving data quality, data protection etc. » Distributing roles and responsibilities in their organization at the operational level (and making certain that the operational data handlers understand the policies and risks) » Acting as focal person for their organization regarding data inventories and tools as their "owners". » Supporting and sharing knowledge with other stewards across organizations. » Assume responsibility for the integrity and quality of the data created or updated in their organization. » Communicating new and changed data requirements to data handlers in their organization » Identification of the data domain stewards for their organization » Communicating concerns, issues and problems with data to the Steering Body	

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
Data Domain Stewards	» Data Domain Stewards are the individuals responsible for harmonizing the collection of one certain type of farmers' data across institutions. They have the responsibility of documenting how the data in their domain is classified (open, sensitive, restricted), secured, the business rules around the data in their domain, audited, and regulated. They are also responsible for implementing related policies. *Overview of responsibilities:* » Define the data and identify assets within their own data domains. This ensures there is no conflict with other data types. » Focusing on the quality of data for a data domain (data type) using user feedback, concerns, questions and internal reporting metrics » Involved/facilitator in cross-organizational resolution of data definition, production, and usage issues for the data domain in question » Escalating well-documented issues to the Steering Body with or without recommendation. » Documenting data classification, compliance rules, and rules for data in their domain. » Create processes and procedures along with access controls to monitor adherence. » Making certain the rules are communicated to all stakeholders of data in that domain » Participating in exchange groups (with other domain stewards) » This includes establishing internal policies and standards—and enforcing those » Monitor data usage to assist teams, share best practice trends in data use, and provide insight into how and where data to help in day-to-day decision-making. » Ensure compliance and security of the data in their domain. Data stewards are responsible for protecting the data—while providing information on potential risks and offering regulatory guidance.	These roles are typically located in the IT department and filled by senior IT or data professionals with expertise on data assets. Data Governance Council members will appoint the coordinators.

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
Data Domain Stewards (Cross-organizational level)	» Data Domain Stewards are the individuals responsible for harmonizing the collection of one certain type of farmers' data across institutions. They have the responsibility of documenting how the data in their domain is classified (open, sensitive, restricted), secured, the business rules around the data in their domain, audited, and regulated. They are also responsible for implementing related policies. » Overview of responsibilities: » Define the data and identify assets within their own data domains. This ensures there is no conflict with other data types. » Focusing on the quality of data for a data domain (data type) using user feedback, concerns, questions and internal reporting metrics » Involved/facilitator in cross-organizational resolution of data definition, production, and usage issues for the data domain in question » Escalating well-documented issues to the Steering Body with or without recommendation. » Documenting data classification, compliance rules, and rules for data in their domain. » Create processes and procedures along with access controls to monitor adherence. » Making certain the rules are communicated to all stakeholders of data in that domain » Participating in exchange groups (with other domain stewards) » This includes establishing internal policies and standards—and enforcing those » Monitor data usage to assist teams, share best practice trends in data use, and provide insight into how and where data to help in day-to-day decision-making. » Ensure compliance and security of the data in their domain. Data stewards are responsible for protecting the data—while providing information on potential risks and offering regulatory guidance.	These roles are typically located in the IT department and filled by senior IT or data professionals with expertise on data assets. Data Governance Council members will designate the data domain stewards.

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
Data Protection Officers (Operational level)	» A data protection officer (DPO) is a security leadership role required by the Data Protection Act. Data protection officers are responsible for overseeing data processors / controllers data privacy and security strategy and its implementation to ensure compliance with DPA requirements. » Overview of responsibilities: » Advising the data controller or data processor and data handlers and stewards on data processing requirements provided under the DPA and the data privacy and security policy. » Ensuring compliance with the DPA. » Facilitating capacity building of staff involved in data processing operations. » Providing advice on data protection impact assessment; and » Co-operating with the ODPC and any other authority on matters relating to data protection. » Monitoring and evaluating the efficiency of the data systems in the organization » Keeping written records (inventory) of the processing activities	MoALFC within the departments, KARLO existing employee, or externally appointed and in general any other data controller or data processor where their activities require regular and systematic monitoring of farmers data
Data handlers (Operational level)	Data handlers are the individuals responsible for collecting the farmers registration data and editing them into data sets according to the outlined standards (privacy, data quality etc.). Overview of responsibilities: » Focusing on consistent protection and classification of data (personal, non-personal, public, internal use …). » Technical handling of personal data and application of data protection and security safeguards as well as guidelines to comply with privacy standards of the Data Protection Act. » Collection of informed consent from farmers for the use of their personal data; archive the collected consent forms for auditing purposes	

ROLES	RESPONSIBILITIES	SUGGESTED ACTOR(S)
Data experts	» Data experts transfer information from hardcopy to digital format. They oversee the entire conversion process, verifying the validity of the information, designing storage platforms, and training staff on document retrieval procedures. » Overview of responsibilities: » Execute all regular transaction processes necessary to maintain records and databases » Perform extracting, importing, and exporting of data in various database applications » Assist in implementation, testing, and validating data and software systems » Perform data analysis of key problem areas to assist in root cause analysis » Audit data on a regular basis to ensure data integrity and quality » Assist with ongoing data architecture processes and governance » Research and collect data to assist with product development and analysis » Train staff as necessary on data operational activities » Perform data reconciliations to identify data anomalies » Escalate data issues needing process re-engineering » Perform data quantitative and qualitative analysis » Assist in preparation of data reports, training materials, business presentations publications, marketing collaterals, and other educational materials	External consultants and trainers
Data subject	The data subjects are the farmers whose data is registered in the Kenya United Agriculture Data Platform (KUADP. Their data rights must be adhered to by the data processors and controllers	Farmers

PILLAR 2

Privacy Standards

Kenya's data protection regulation provides the framework for the legal collection and processing of farmers' personal data. When it comes to the different farmers' data types collected in use case 1, it can be noted that while some are personal, some are not, and some might become personal depending on the context of their use:

» Farmer national ID number	» Personal data
» Name	» Personal data
» Mobile number	» Personal data
» Address	» Personal data
» Size of land	» Personal data depending on the context
» Value chains grown	» Personal data depending on the context
» Yield of value chains produced	» Non-personal data
» Income from agricultural output	» Personal data
» Type of inputs (i.e. subsidies) received	» Personal data depending on context
» Quantity of inputs received	» Non-personal data
» Price of inputs received	» Non-personal data
» Geographic location of inputs received	» Personal data depending on the context

According to the DAPA, for the data types falling under the category of personal data, there needs to be a legal basis for their processing (section 30). Looking at the eight legal bases for the lawful use of personal (farmers) data that data controllers and data processors in the agriculture sector have to consider, it becomes apparent that different legal bases might apply to the different personal data sets under use case 1.

Privacy Standards

Namely, the legal bases for processing personal (farmers) data are the following:

1 Consent: The farmer has given consent to the processing for one or more specified purposes.

2 Contract: The processing of data is necessary for the performance of a contract to which the farmer is a party or to take steps at the farmer's request before entering into a contract with the data controller or data processor.

3 Legal obligation: For compliance with any legal obligation to which the data controller is subject.

4 Vital interests: The processing is necessary to protect the vital interests of the farmer or another natural person.

5 Public task: The processing is necessary for performing a task carried out in the public interest or in the exercise of official authority vested in the data controller.

6 The performance of any task carried out by public authority: The processing is necessary for the exercise, by any person in the public interest, of any other functions of a public nature.

7 Legitimate interests: These interests are pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the farmer.

8 Historical, statistical, journalistic, literature and art or scientific purposes.

No single basis is considered "more suitable" or more important than others. Which basis is most appropriate to use will depend on the exact purpose defined, for example, by the MoALFC, KARLO, KNBS and their relationship with the data subjects, in this case, the farmers. To illustrate, should a public authority need to process personal farmers' data to perform its official task, there might be some limitations with regards to a legitimate interest.

Privacy Standards

In light of having identified the data types falling within the scope of the DPA and having discussed the legal basis for their use, their governance in terms of privacy protection will be guided by six key standards which help ensure compliance with the law. The six standards are outlined and discussed in detail in the following:

Standard 1: Ensure informed consent from farmers (data subjects)

For processing to be lawful under the Data Protection Act, it is necessary to identify (and document) the lawful basis for the processing. There are eight lawful bases listed in section 30 of the Act, and consent is one of them. Consent means any manifestation of express, unequivocal, free, specific, and informed indication of the data subjects (in this case the farmer) wishes by a statement or by clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.
Personal data is any information relating to an identified or identifiable person such as:

- A name and surname
- A home address
- An email address
- An identification card number
- Location data (for example, the location data function on a mobile phone)
- An Internet Protocol (IP) address

If the consent should legitimize the processing of special categories of personal data, like sensitive personal data, the information for the data subject must expressly refer to this. "Sensitive personal data" means 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.

According to DPA, consent can only be an appropriate lawful basis if a data subject (the farmer) is offered control and is offered a genuine choice about accepting or declining the terms offered or declining them without detriment. When asking for consent, a data controller (e.g., the MoALFC) or data processor (e.g., the KNBS or KALRO when using data on behalf of the ministry) has the duty to assess whether it will meet all the requirements to obtain valid consent. If consent is obtained in accordance with the DPA then data subjects (the farmers) will have control over whether their personal data will be processed.

Privacy Standards

Section 32 of the DPA states that a data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose. Therefore, informed consent is required when processing personal data. Farmers' consent must be based on their understanding of the processing activities (e.g., collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) and its implications on their rights. Data controllers or data processors have an obligation to ensure that there is accurate and full information regarding the nature of personal data to be processed, the specific purposes of the processing of data should be clearly stated, the recipients of possible transfers, as well as farmers' rights (e.g., right to data portability, right to erasure / to be forgotten).

Where the processing is based on consent, farmers have the right to withdraw their consent, which, in effect, operates as a right to stop the processing. The withdrawal of consent shall not affect the lawfulness of processing based on prior consent before its withdrawal. Finally, any consequences of not consenting to the processing in question and any relevant information must be provided to farmers to enable them to give informed consent.

In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Data controllers and data processors must obtain new and specific consent if the purpose for data processing has changed after consent was obtained or if an additional purpose is intended. In this case, the information to be provided will focus on what is needed in the specific context in relation to the purpose. Any consent obtained prior to the commencement of the DPA and is compliant with the provisions of the Act will continue to be valid.

Informed consent should provide data subjects (farmers) with the practical means to understand and effectively control who has access to data about them and how it is stored, used, and shared. It must be given voluntarily without coercion, with sufficient disclosure to enable reasoned judgment, and with the capacity to make a legally binding commitment. Typically, written consent documentation includes an informed consent signed by the farmer. Broad but vague statements should be avoided, and clear and plain language should be used.

Privacy Standards	
Standard 2: Comply with farmers (data subject) rights	Standard 3: Notify in case of breach
Farmers have a right to data portability. This means that they are entitled to request copies of their registration data in a readable and standardized format. This means farmers should be able to retrieve their individual data in both processed (cleaned) and unprocessed form for storage or use in other systems, except for the data that has been made anonymous or aggregated and is no longer specifically identifiable. They have the right for this data to be rectified and returned to them. Moreover, farmers have the "right to be forgotten." This new right set out by the DPA is evidence of the data subject being in the driving seat when it comes to the use of their data. The meaning of the right to be forgotten is that farmers can now request that their data be deleted, destroyed, and erased. Practically, this can mean that the agricultural stakeholders processing farmers' registration data will have to perform wholesale reviews of processes, system architecture, and third-party data access controls. In addition, archived data may also need to be reviewed and deleted.	Section 43 of the DPA requires data controllers and processors to give notice to the Office of the Data Protection Commissioner (ODPC) in the event of a data breach and to further give notice to the data subject (farmers) if the data that has been breached can identify them. The law also establishes timelines within which this action should be undertaken. The ODPC has to be notified within 72 hours if the breach is discovered in a timely fashion, or 48 hours if the breach was discovered late. This means that the stakeholders involved in processing farmers' registration data will have to urgently revise their incident management procedures and consider steps for regularly testing, assessing, and evaluating their end-to-end incident management processes in the situation of a data breach, where encryption safeguards were adopted, the DPA exempts the data controller or processor from notifying affected farmer. However, this does not mean that data processors and controllers can afford to be complacent, as the exemption may not apply when weak encryption has been used.

Privacy Standards

Standard 4: Follow Privacy-by-Design

Privacy-by-design is both a broad concept and a specific requirement of the DPA. In simple terms, this means data privacy has to be considered when technological tools are designed and procedures for collecting and handling data setup. The rationale is that it's too late to start thinking about it once personal data is collected. There is a range of privacy-by-design best practices, including the development of data privacy and security policy, sound anonymization and pseudonymization methods, and the carrying out of Data Protection Impact Assessments (DPIA). These concrete measures will be discussed more in-depth in pillars 3 and 4 of the data governance framework. As a general guidance on how to adhere to the privacy-by-design standard, the following six key practical steps should be undertaken by each actor involved in the collection and processing of farmers' registration data[1]:

» *Be proactive, not reactive; preventative, not remedial:* Put simply, this means making privacy a key objective to always follow. So before designing any system and process for handling data, it is essential to figure out what privacy risks the handling of the data will create. Based on this assessment, the necessary steps can be taken to minimize or eliminate those risks and build these steps into the system and processes.

» *Design with privacy in mind:* This step means building privacy protections into every system used for the collection and processing of farmers' registration data from the outset. A key example would be a database of phone numbers collected from farmers during the registration process. To follow the privacy-by-design standard in this context, the database would be created so that, at the time a phone number is added, it automatically generates an expiry date. When a record reaches this date, it should automatically be deleted, or at least automatically blocked from future use until manually reviewed. In overall, it can be adopted as a design standard / pre-requisite when writing Terms of Reference for procurement of new systems as a mandatory / desired security feature of a system.

[1] Derived from the privacy-by-design framework of Dr. Ann Cavoukian, former Information and Privacy Commissioner for the Canadian province of Ontario

Privacy Standards

- *End-to-end security:* This step entails keeping farmers' data secure at every point, from collecting it to using it to disclosing it to destroying it. Some of the practical measures include: (i) using encryption where appropriate, (ii) using a range of security measures, including physical and electronic restrictions (such as passwords) and organizational restrictions (such as giving different staff members different and appropriate levels of access to data), and (iii) monitoring access points to data so that breaches can be swiftly identified. These security measures are ideally detailed in the data privacy and security policy to inform both the ODPC and farmers.
- *Visibility and transparency:* The idea behind this step is that data subjects, i.e., registered farmers, should be kept informed and that this will not only increase their trust in the data governance framework but also ensure the accountability of data processors and controllers for the way they handle farmers' registration data. Central elements here are to (i) make the contact details of every data processor and controller, as well as their DPOs publicly available, (ii) communicate the purpose(s) for data collection as well as the legal basis under which the data is processed, and (iii) be transparent about who data is shared with, how long the data is kept and whether automated decision-making is applied to the data in question.

These key steps should also be mirrored in the data privacy and security policy discussed further in pillar 3 and complemented by the other privacy standards (pillar 2).

Privacy Standards	
Standard 5: Create inventories for data processing activities	**Standard 6: Appoint DPOs**
At the highest level, a personal data inventory is a record of all personally identifiable farmers' data and related processes. Following the provisions set out by the DPA, data processors and controllers will have to take steps to demonstrate they know what data they hold, where it is stored, and who it is shared with by creating and maintaining an inventory of data processing activities. Data handlers will have to work closely with the DPOs to ensure all necessary bases are covered. A thorough system for maintaining inventories needs to be implemented. There are several elements that should be included in any thorough personal data inventory, including: » Types of data (e.g., "farmer phone number") » Where to find the data within the system (e.g., "Kenya United Agriculture Data Platform (KUADP") » Data subjects (e.g., "farmers") » How the data was collected (e.g., "USSD survey") » How the data is used (e.g., "allocation of e-vouchers") » How long the data will be stored » Who has access to the farmers' data? » Who owns the data (e.g., MoALFC, KALRO, Counties, Farmers Organizations) » Policies for deleting or preserving the data	The Act makes provisions for the designation of Data Protection Officers (DPOs). Although this obligation is not mandatory, it is highly recommended. DPOs can be staff members and may perform other roles in addition to their roles. The shareholders involved in use case 1 could share a DPO. The contact details of the DPO must be communicated to the ODPC.

Policies and Guidelines

Policies are a deliberate system of directions for decision-making and the achievement of rational outcomes. A policy is also a statement of intent and is implemented as a procedure or protocol. Policies are generally adopted by a governance body within an organization. They can assist in both subjective and objective decision-making. A guideline is a statement by which to determine a course of action. A guideline aims to streamline particular processes according to a set routine or sound practice. Guidelines may be issued and used by any organization (governmental or private) to make the actions of its employees or divisions more predictable and presumably of higher quality. A guideline is, therefore, similar to a rule. In the following section, the most important policies and guidelines for the governance of farmers' registration data to be developed under the data governance framework are outlined:

Internal data governance policy	External (open) data policy
The internal data governance policy will document a set of guidelines and tools for ensuring that farmers' data are managed consistently and used properly. Such guidelines and tools typically include individual policies and instruments for data quality, access, security, privacy and usage, as well as roles, and responsibilities (as outlined in Pillar 1) for implementing those policies and monitoring compliance with them. It enables the tools to be used consistently by the data handlers and data stewards and updated as necessary, so they can serve as a trusted reference when data-related challenges (e.g., data quality) and opportunities (data sharing activities) emerge. The policy-approving group for the internal data governance policy is the Data Governance Council. **Examples of internal data governance policies in Annex 9.1**	*External (open) data policy:* A public-facing (open) data policy is an important indicator of the data governance maturity of an organization, in this case, the MoALFC. An (open) data policy is based on a clear understanding of the characteristics of key data, i.e., data types, data ownership and data use roles (as outlined in the internal data governance policy). The policy-approving group for the internal data governance policy is the Data Governance Council. **Guide for (open) data policy in Annex 9.2**

Policies and Guidelines	
Data Protection and Security Guidelines	Data Retention Policy
A Data Protection and Security Guideline is a statement that sets out how an organization protects personal data. It is a set of principles and rules that informs how it will ensure ongoing compliance with data protection laws. Moreover, as mentioned under pillar 2, one of the central aspects to implementing the privacy-by-design standard is developing a data privacy and security policy. Having such a policy does not in itself achieve privacy-by-design. However, it plays several key roles in following both the concept of privacy-by-design and the related requirements of the DPA: » Drafting a data privacy and security policy can raise points that need to be covered by privacy procedures and data processing. » Many of the key measures in achieving privacy-by-design can be detailed in a policy. This helps demonstrate compliance and commitment to the privacy-by-design standard set out by the DPA, both to ODPC and farmers. » Some of the requirements of a privacy-by-design approach involve keeping farmers informed about data handling. A data privacy and security policy are the best way to do this. **Examples of data protection and security guidelines in Annex 9.3**	A data retention policy is a set of guidelines that will help the MoALFC keep track of how long farmers personal data must be kept and how to dispose of this data when it's no longer needed. Once a set of farmers' data completes its retention period, it can be deleted or moved as historical data to secondary or tertiary storage, depending on the consent agreement with the farmers. A streamlined data retention policy offers great benefits: (i) it helps ensure compliance with industry guidelines and regulations. This avoids expensive civil, criminal or financial penalties stemming from non-compliance; (ii) it assists in discarding outdated and duplicated data, making it easier to find relevant information; (iii) it makes room for more storage space as it is not necessary to retain data longer than needed. This frees up storage space to make room for new data. The policy, therefore, lowers storage costs and increases speed. **Data retention policy template in Annex 9.4**

Tools

Data governance tools aid in the process of implementing the policies and standards set out in pillars 2 and 3. The data handlers and data stewards, especially, benefit from the existence of these tools to guide their actions. For all the tools discussed below, it is important to assign ownership. This means that an owner is identified and assigned responsibility for their content and maintenance. These owners also inform the Steering Body regarding the usefulness of the tools and about challenges encountered in their usage. Usually, Data Steward Coordinators take over this role.

Data privacy and security practices

Data privacy practices cover anonymization and pseudonymization techniques that should be documented, regularly monitored, and reviewed to ensure their rigor in support of farmers' privacy. Pseudonymization is a procedure where any identifying characteristic of personal data is replaced by one or several artificial identifiers, the so-called pseudonyms. These can range from just one pseudonym to several replaced fields or one pseudonym per replaced field, which does not allow the data subject to be directly identified. Pseudonymization is one of the techniques that support compliance with data protection obligations, especially in relation to the principle of "data minimization". Data minimization refers to the practice of limiting the collection of personal data to that which is directly relevant to accomplish a specified purpose and ensuring that this data is not retained longer than necessary. Anonymous data, on the other hand, is information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Therefore, data anonymization refers to the process of removing direct and indirect personal identifiers. This includes but is not limited to any information that may allow for the identification of an individual, such as an address, phone number, picture, date of birth, etc. Data anonymization uses various de-identification methods to ensure that individuals are no longer identifiable. Anonymization is the strongest form of privacy protection available as it irreversibly scrubs any information that may serve as an identifier. It typically exempts data from data protection compliance requirements related to personal data. Anonymized data, therefore, no longer falls inside the DPA scope of application. As a rule of thumb, public-facing datasets should be anonymized, and personal data included only if necessary, to preserve the data's analytic potential, scientific utility, or benefit to the farmer, subject to prior informed consent and rigorous risk assessment.

There is a variety of (open-source) **tools and programs for data pseudonymization and data anonymization**. Below a list of the standard techniques is provided[1]. It is important to document these practices to demonstrate due diligence in response to any inquiries regarding data privacy either by data subjects (farmers).

[1] Based on the guide provided by the data science consultancy Record Evolution at: https://www.record-evolution.de/en/data-anonymization-techniques-and-best-practices-a-quick-guide/

Tools

- *Directory replacement:* The directory replacement technique is about making changes to the names of individuals within the data but keeping consistent relations between other variables. For example, if an address and an ID are used to identify an individual, the information that directly identifies the individual, the ID, should be stored in a separate location. This allows the data to be pseudonymized. To anonymize, the separately stored data that identifies the individual should be deleted.
- *Scrambling or Shuffling:* This method is simply about mixing of letters or digits in the personal data. For instance, #61785 may become #76815. In a perfect scenario, the process is irreversible so that the original data cannot be retrieved from the shuffled or scrambled data.
- *Generalization:* This method follows the rational of reducing the granularity of the data. Therefore, disclosed data is less accurate than the original data and hence makes it difficult, if not impossible, to retrieve the exact values associated with an individual.
- *Masking out:* This technique is a way to create a fake but a realistic version of the data. It allows for hiding part of the data by placing random characters or other data instead. One can pseudonymize by masking identities or important identifiers and still be able to identify the data without manipulating the actual identities. A common example includes the masking of credit card information that is then shown in the form XXXX XXXX XXXX 1165.
- *Blurring:* Like generalization, this method reduces the precision of the disclosed data to minimize the possibility of identification. An approximation of data values is used instead of the original identifiers, making it hard to identify individuals with absolute accuracy. To illustrate, an individual might be identifiable by an exact account balance at a particular moment in time. If one now adds small random values to this overall balance, this does not produce a significant error in the data but provides anonymity for the affected individual.

Tools

- *Data encryption:* This method changes the personal data into another form or code so that data that is categorized as sensitive is replaced with data in an unreadable format. Certain authorized users have access to a password that allows them to view the data in its original format. In many cases, encryption can provide an appropriate safeguard against the unauthorized or unlawful processing of personal data, especially in cases where it is not possible to implement alternative measures. Data encryption also provides a safe harbor from breach notifications as it permits the securing of remote locations and setting the baseline for safe outsourcing and licensing of data. Likewise, it can also avoid that service provider's access or inadvertently exposing data.
- *Nulling out:* The basic function applied in this this technique is removing and deleting sensitive data from the data set. All elements of sensitive information, such as the farmers' name, address, or phone number, become null values.
- *Substitution:* By definition, this technique replaces the contents of a database column or row with data from a predefined list of fake data to ensure that the data is not traced back to the individual. The key characteristic of this method is that it maintains the integrity of the original information.
- *Number and date variance:* This anonymization technique comes into play when dealing with numeric and date columns. In this scenario, each value in a column is altered by a random percentage of its actual value. The data is modified to the point that it can no longer be traced back to its original form.

Data security practices are about helping to protect farmers' data from unauthorized access from malicious actors. This includes IT access and security controls, appropriate technological, and physical controls as outlined below[2]:

Administrative controls: Beyond having an underlying data security policy that outlines actions that are permitted, the penalties in case of a violation, etc. (as discussed in pillar 3 of the framework), a sound supervisory structure is an essential part of administrative controls. Hence Data Coordination Stewards should be responsible for the activities of their staff, i.e., data handlers.

[2] https://www.netwrix.com/data_security_best_practices.html

Tools

Permission controls: Access permissions should only be attributed in strict accordance with the principle of least privileges. Possible permission levels to be granted with regards to accessing farmers' data on the National Agriculture Data Platform include:

Full Control	The user can read, execute, modify and delete data; assign permissions; and take ownership.
Modify	The user can read, write and delete data.
Read and Execute	The user can run the executable data.
Read	The user can read but not modify the data.
Write	The user can read and modify the data but not delete it.

Different permissions may apply to different types of data. Usually, users should not be prohibited from copying and storing sensitive personal data locally but forced to work with the data remotely. The cache of the client and server system should both be comprehensively cleaned after a session ends or a user logs off, or else encrypted RAM drives should be relied upon. Sensitive personal farmers' data should, in the best-case scenario, never be stored on a portable system. All systems holding personal farmers' data should have a login of some kind and conditions set to lock the system if questionable usage happens.

Access control lists: An access control list (ACL) is a list stating who is allowed to access what type of data and at what level. It can be an internal part of the National Agriculture Data Platform operating system or part of one or several of its applications. For instance, a specific function of the platform might have an ACL that lists which users have what permissions regarding the function. ACLs can be based on whitelists or blacklists. A whitelist encompasses items that are allowed, e.g., a list of data types that users are permitted to access. Blacklists are lists of actions that are prohibited, such as access or download of certain data types.

Tools

Security devices and methods: Certain devices and systems help to further restrict access to data. In the following, a list of the most commonly implemented ones is provided:

- *Data loss prevention (DLP)* — DLP systems monitor the servers, workstations, and networks to ensure that sensitive data like farmers' data is not deleted, removed, changed, or copied. They also monitor who is using and transmitting the data to identify unauthorized actions and use.
- *Firewalls* — a firewall is one of the first lines of defense in a system as it isolates one part of the system from another. Firewalls can be standalone, or they can be included in other infrastructure devices, such as servers and routers. They can be hardware or software solutions. Firewalls filter out undesirable traffic and users from entering an organization's system, preventing data leaks to malicious third-party servers by malware or hackers.
- *Proxy server* — these devices have the role of negotiators for requests from user software requesting access to resources from other servers. A user connects to the proxy server, requesting some service (e.g., access to farmers' data type Y); the proxy server evaluates the request and then allows or denies it.

Physical controls: Physical security is in many cases overlooked in debates about data security. But if one has a poor policy on physical security, this can lead to a full compromise of data or even platforms. Hard drives or other sensitive components of the National Agriculture Data Platform that store farmers' data can be removed and accessed by malicious actors. Thus, every workstation should be locked down in a way that it cannot be removed from the work area. A good practice is also to integrate a BIOS password to prevent malicious parties from booting into other operating systems using removable data. BIOS password is authentication information required to log into a computer's basic input/output system (BIOS) before the machine will boot up. Moreover, encryption keys should only be stored in places where they cannot be accessed easily (especially simultaneously with the encrypted data). In fact, it is best not to store passwords physically at all.

Laptop security: With laptops, the greatest problems are loss and theft, either of which can enable malicious actors to access the data on the hard drive. Full-disk encryption should be used on every laptop holding sensitive farmers' data of the Kenya United Agriculture Data Platform (KUADP. Also, using public Wi-Fi hotspots should be avoided unless a secure communication channel such as a VPN or SSH is used.

Tools

Mobile device security: Mobile end devices can import viruses or other malware into an entity's network and extract sensitive farmers' data from its servers. To counter these threats, mobile devices have to be controlled very strictly. Devices that are allowed to connect to the entity's network should be checked for viruses, and removable devices should be encrypted. As an overall strategy, it is vital to focus on the data, not the device it resides on. Smartphones often contain sensitive data, yet less security applies to them than to laptops that contain the same data.

Network Segregation of the Kenya United Agriculture Data Platform (KUADP: Network segmentation involves segregating the platform into functional or logical fragments called zones. Every zone can be assigned different data categorization guidelines, set to an appropriate security level. Segregating a network limits the potential damage if a single zone should be compromised. It basically separates one target into many, leaving malicious parties with the choice to either treat each segment as a separate network or try to attack one and then attempt to attack the others – neither of the two possibilities being attractive options.

Video surveillance and locking: To sport unauthorized people trying to misuse farmers' data by directly accessing servers, archives, etc., the technical infrastructure of the Kenya United Agriculture Data Platform (KUADP should be adequately secured by video cameras. Moreover, the work area and equipment of staff handling the data should be secured before being left unattended.

Video surveillance: Monitoring all critical facilities of the technical infrastructure of the Kenya United Agriculture Data Platform (KUADP by video cameras with motion sensors and night vision is essential for spotting unauthorized people trying to steal or access farmers' data via direct access to file servers, archives or backups, as well as spotting people taking photos of sensitive data in restricted areas.

Tools

Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) should be conducted when a new project that is likely to involve "a high risk" to other people's personal information, like the centralization of farmers' registration data on a unified platform, is commenced. Carrying out a DPIA is also one of the most important ways to demonstrate to the ODPC that compliance with the DPA is ensured and best practices for data security and privacy are being followed.

To put it shortly, a Data Protection Impact Assessment (DPIA) is a way to systematically and comprehensively analyze data processing and identify and minimize data protection risks (potentially) resulting from the processing. DPIAs should consider compliance risks but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether physical, material or non-material. To assess the level of risk, a DPIA must consider both the likelihood and severity of any impact on individuals.

Hence, a DPIA should contain the following elements:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights of farmers
- The measures envisaged addressing the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the DPA, considering the rights and legitimate interests of farmers

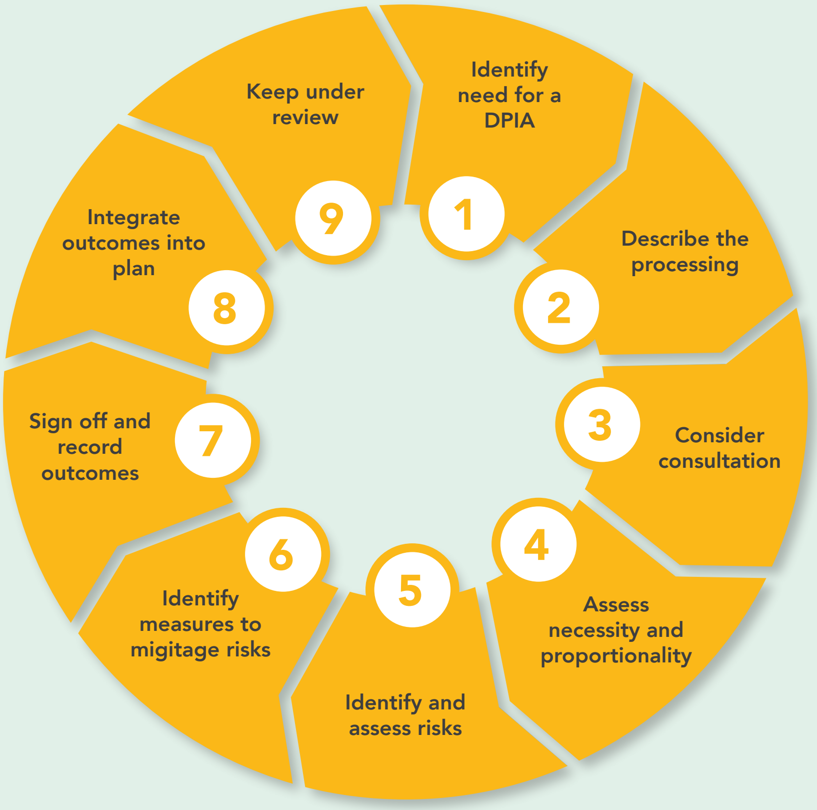
A DPIA does not have to indicate that all risks have been eradicated. But it should help document them and assess whether and remaining risks are justified. DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance and financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals.

Tools

How do we carry out a DPIA?

The DPIA must be prepared before beginning any data processing activity, ideally together with the Data Protection Officer and involved stakeholders, and run alongside the planning and development process.

It should include these steps:


1
Identify need for a DPIA
2
Describe the processing
3
Consider consultation
4
Assess necessity and proportionality
5
Identify and assess risks
6
Identify measures to migitage risks
7
Sign off and record outcomes
8
Integrate outcomes into plan
9
Keep under review

The United Kingdom's (UK) Information Commissioner's Office (ICO) has prepared a Data Protection Impact Assessment template which serves as an excellent guide through the process of determining whether data processing activity requires a DPIA and helps determine what safeguards should be implemented to conform to privacy standards.

The template is provided in the Annex 9.5 or can be looked up here; The Kenyan Office of the Data Protection Commissioner (ODPC) is currently also development a template that will be accessible here, once published.

Tools

Informed Consent Form

As discussed in pillar two, informed consent from farmers to the processing of their personal data is best recorded in the form of a contractual agreement. The agreement must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. In summary, an informed consent form should cover the following topics:

- Purpose of the collection of data as well as who is undertaking the processing. That means that the data controller or data processor (e.g., the ICT State department of the MoALFC, the Counties, KALRO, the KBNS) must identity itself, and name any third party who will be relying on the consent.
- Description of the types of data to be collected and processed.
- Voluntary invitation to participate and ideally give farmers the option to have their identity anonymized or otherwise protected.
- Procedure for discontinuation or withdrawal of consent (including any constraints to withdrawal, e.g., if personal data has been analyzed, shared, or published).
- Benefits of participating (directly to the farmers and indirectly to society or others).
- Specific purpose for which personal data is being collected as narrowly and precisely defined as practically possible.
- Explicit permissions and limitations concerning the use of personal data (particularly for activities involving archiving, transfer, re-use or sharing of PII, or follow-up).
- Who will have access to personal data, what security measures will be taken?
- Any reasonably foreseeable risk of identification noting probability of potential harm (e.g., physical, psychological, economic, or social).
- Distinguish personal data that might have different disclosure risks (e.g., interview transcripts, audio recordings, videos, pictures).
- How personal data will be used in datasets.
- Farmer’s signature and date of signing.

Tools

Moreover, the consent form should confirm and allow the farmer to respond to points such as:

- the farmer has read and understood information about the collection of his/her data
- the farmer has been given the opportunity to ask questions
- the farmer voluntarily agrees to participate in the data collection process
- the farmer understands he or she can withdraw their participation or consent at any time or by a specific deadline, without giving reasons and without penalty
- the farmer acknowledges the nature of the personal data that will be collected and permits it to be used in the manner disclosed
- the farmer accepts the implications to their privacy and the potential risk of harm
- provide a specific individual and title with whom to follow up for any clarification, concern, or complaint
- confirm that the farmer will be given a copy of the form, and the data controller-data processor will retain the signed original

Finally, the lawful basis of consent is likely to overlap with other lawful bases. For example, a data controller and or data processor may have a statutory obligation to process certain personal data. However, the data controller and/or data processor may wish to process more personal data than is required under the statute for a specified purpose. In this case, there is a need to adopt hybrid models, where consent is sought for any processing that may be deemed to be beyond the statutory requirement and the data subject advised of the statutory requirement and its limitations with respect to the processing activity

The Office of the Data Protection Commissioner (ODPC) has developed a template on informed consent; another informed consent template and guides can be found in Annex 9.7

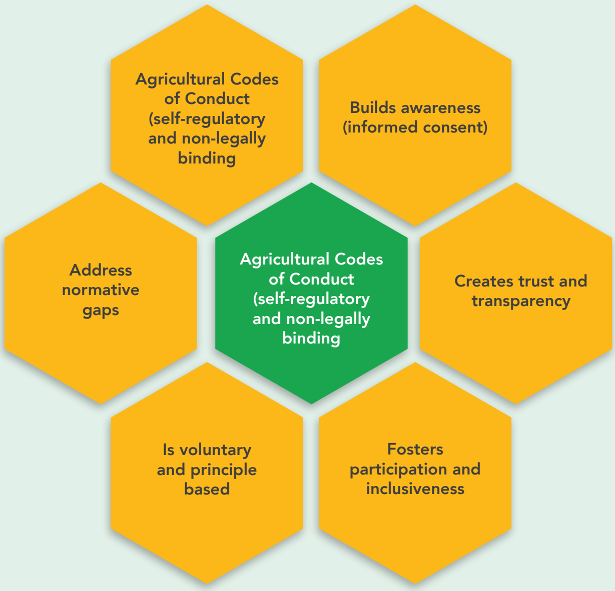
Tools
Relevant references documents and links ODPC guidance note on consent ICO guidelines on consent CGIAR Responsible Data GUIDELINES GDPR consent Berkley Informed consent Berkley Informed consent guidelines Berkley Instructions for signed versus unsigned informed consent

Agricultural Code of Conduct

As highlighted by the GODAN initiative, farmers' data travels from the farm through many other actors (e.g., extensionists, advisory service providers, farmers' associations, financial service providers, government, etc.), before coming back to the farm – aggregated and combined and in the form of services. Such data flows potentially open up access to sensitive farmers' data that should only be shared with certain actors under certain conditions or needs to be anonymized to mitigate negative impacts on farmers' legitimate interests and privacy rights. This holds especially true for smallholder farmers, whose data often coincides with household data and sensitive personal data but are often in the most vulnerable position to claim their data rights.

While there are policies and laws that govern personal data and data rights, regulations still do not comprehensively encompass all farmers' data flows. Agricultural Codes of Conduct have started to emerge as a self-regulatory remedy to fill the legislative void, setting common standards for data sharing agreements based on the needs of communities while guaranteeing an even distribution of benefits between agricultural chain actors. Codes provide principles that the signatories agree to apply in their contracts and a conceptual basis for general, scalable guidelines for everyone dealing with the production, ownership, sharing, and use of data in agriculture, i.e., farmers' data.

Illustration 2: Agricultural Codes of Conduct Rationales


Agricultural Codes of Conduct (self-regulatory and non-legally binding
Builds awareness (informed consent)
Address normative gaps
Agricultural Codes of Conduct (self-regulatory and non-legally binding
Creates trust and transparency
Is voluntary and principle based
Fosters participation and inclusiveness

Tools

A best practice reference project for topics to be covered by Agricultural Codes of Conduct stems from GODAN, which is a joint initiative with CTA and GFAR, proposed the following clauses that could be included in an Agricultural Code of Conduct:

1. Definitions
2. Ability to control and access
3. Consent for collection, access, and control
4. Purpose Limitation
5. Notice
6. Transparency and Consistency
7. Rights of the Data Originator
8. Right to Benefit
9. Disclosure, use, and sale limitation
10. Data retention and availability
11. Contract Termination
12. Unlawful or anti-competitive activities
13. Data protection safeguards
14. Liability and Protection of IP rights
15. Simple and Understandable Contracts
16. Certification Schemes
17. Compliance with National and International Laws

Despite Agricultural Codes of Conduct being voluntary and not legally binding, they nevertheless have the potential to contribute towards major cultural shifts. Codes of Conduct provide a solid framework for best practice in data management through the engagement of all stakeholders (including, and especially, farmers) in open dialogue to find solutions that address the needs of everyone involved.

GODAN's Codes of Conduct development toolkit for the agricultural sector can be accessed via Annex 9.6.

Tools

Data Sharing Agreement HOW TO-Guide

A data-sharing agreement is a contract between two or more organizations about how to share data. It will define what data is being shared and for how long, and any restrictions on its use. Data sharing agreements confer rights and responsibilities between the different organizations and stakeholders and provide certainty for the different uses of relevant farmers' data. If the data is already published, then a sharing agreement may not be needed. To minimize multiple accesses to primary farmers' data, the National Agriculture Data Platform would be the single source of externally requested farmers' data. This implies that all incoming requests for farmer data would be processed in the platform, and the data would be provided from there. In this case, the platform would source this data from primary systems.

For use case 1 and the sharing of farmers' registration data, data sharing agreements will potentially be required between:

- MoALFC – KALRO
- MoALFC-KCEP-CRAL
- MoALFC-EAGG
- MoALFC-Counties
- KCEP-CRAL-Counties
- Counties-KENAFF
- KEPHIS-KENAFF

HOW TO-Guide for developing a data-sharing agreement with third parties

Key points to cover with a data-sharing agreement

- A description of the entities signing the agreement
- A statement summarizing the purpose of the agreement, i.e., what are the objectives of data sharing
- The main contacts in each organization for queries about the data – e.g., the data domain stewards
- Any financial agreement that may cover how both costs and benefits are distributed

Tools

Define what data will be shared

- Specify the name, description, and any unique reference number to identify the data to be shared
- If the data is described in a data catalogue accessible to both parties, it might be described most easily and clearly by referencing its catalogue entry.
- Determine the structure (e.g., attributes, parameters, etc.) of the data that will be shared
- Time period the data covers(if appropriate)
- Format of the data and data quality required
- Define the source of the data (one organization or from a combination of different sources (for the latter, intellectual property rights could have implications for how the data can be shared and used))
- Information about whether the contributing sources know that the data will be shared
- Define if the sharing is a one-off transfer or if updates are to be made. If updates are required: Would they be as necessary corrections to the data? Would they be additions to the data? How regularly can they be made? If this is a one-off transfer of data, when will the data be provided?
- Clearly outline roles and responsibilities. Where possible, include name and contact details of organization representatives as well as a description of roles and responsibilities, e.g., who will prepare and update data, who will monitor implementation of the agreement, who to contact to resolve disputes, etc.

Determine how data will be shared

- Modalities for sharing the data between the parties (e.g., among MoALFC, KALRO, and Counties)
- Define where the data is going to be stored
- Define who is responsible for hosting the data (in this case, KALRO)
- Specify the security measures to be taken to secure sensitive data
- Determine how long the data is going to be shared for
- Define if data copies have to be destroyed at the end of the agreement and how this will be verified

Examples of how data can be shared, supplied and hosted

- Open access publication
- Deposited with a special data center, data archive or database
- Made available online via a project or institution website
- Made avaialable via a secure, online interfae that provides limited access to it
- Made avaolable at a secure pysical location
- Deposited in an institutional repository
- Submitted to a journal to supplement a publication

Tools

Specify how data will be used

This section focuses on specifying what the data can be used for. This can be linked to the data's source. Where data comes from more than one source (i.e., different organizations) you will need to check with the original data providers whether you have the right to share the data and confirm any restrictions on use.

- Permissions needed for each party describing how they can use the data
- Requirements to follow in order to retain those permissions, e.g., to attribute the source of the data
- Restrictions which might be setup to limit the use of the data, e.g., sharing data with third parties
- Define whether the data can be used in commercial products and services
- Consider whether permissions are needed (e.g., from third parties or individual consent) to share or use the farmers' data
- If a data license is to be used, define which one

Derived data

This section focuses on products that might be produced that incorporate data that has been shared:

- Define who will have rights over or have access to what has been produced using the data that has been shared
- Specify if derived data should be published and, if so, what licensing restrictions might apply to how that data is published for reuse by others

Since the data that is going to be collected, used, and shared in the Kenya United Agriculture Data Platform (KUADP is about farmers' personal data, clauses should be added to specify:

- How the data will be secured in transit to third parties and while in their control
- The retention period for the data
- Imitations to third-party use of the data

Tools

Moreover, the data-sharing agreement should contain provisions, demanding for:

- An updated data catalogue
- Scheduling and resourcing updates
- Quality checks to ensure that the provided data is suitably accurate, e.g., through feedback from the data user/recipient on its quality, completeness, format, timeliness, etc.
- Confirmation that the data user/recipient is complying with the terms of your agreement
- Resourcing any changes to how the data is managed based on user feedback
- The provision of information to the data users/recipients about any planned changes to the scope, provision, or availability of the data in future

A template for data sharing between a private sector and a public sector entity can be found in Annex 9.8.

Data Catalogue

The centralized data catalogue gives an overview of the different types of farmers' data collected for use case 1. The catalogue thus provides a reference point for understanding what data is being collected, in which formats, who are its data stewards and handlers, where the data is stored and who has access to it. A catalogue can also be referred to as a data register, dictionary, or a data inventory.

A good data catalogue should have an owner responsible for its creation and ongoing maintenance (when data fields are changed, removed, or added), e.g., KALRO. Moreover, the catalogue presents an important basis for the development of data policies (internal and external) and the technical setup of the National Agriculture Data Platform, such as the development of software tools that will be used to build the platform. This would provide a centralized management of data lineage.

The catalogue can also be helpful in identifying personal data that is used and shared within the platform for farmers' registration, therefore, informing the inventory for personal data processing activities (pillar 2). A centralized data catalogue effort and aligned methodology will help determine which data domains/types will receive priority and data governance resources (staff time to document data processes, clean data, create data outputs and reports, and make decisions about data, etc.).

A data catalogue template can be found in Annex 9.9.

Tools

Data License Register

Once the legal basis for the collection and processing of farmers' data is clarified and the key data processes documented, a data license register can be developed. A data license register lists data types and accompanying licenses and helps to track licenses attached to different data types. This can be useful in supporting staff in determining whether data can be shared and under what conditions when external stakeholders make requests to access data.

Templates for Data License Register can be found in Annex 9.10

PILLAR 5

Processes and Procedures

In order to ensure a transparent and responsible way of handling farmers' personal data, standards and procedures need to be defined to control the data handling at all levels. These levels include the collection, processing, documentation, sharing, and dissemination of personal data. The processes and standards which need to be installed are outlined in the following. All stakeholders acting as data controllers, data processors, or third-party users have to be informed about them.

Data Flow Mapping

Where does the data come from? How is it transmitted and moved across the platform? Where is it stored? How is the data ultimately used internally (e.g., reports)? How is it used externally (e.g., sharing with stakeholders)? Data flow mapping is a step-by-step process where the involved stakeholders construct a graphic that documents data management processes: identification of data sources, data collection processes and tools, data collation systems and tools, data analysis, data reporting, and data use. Data flow mapping is useful for understanding how data quality, data management, and data assessment work together.

The map enables one to document processes and tools that comprise data management. Visualizing a data management system, including stakeholder involvement, allows programs to better understand their systems and identify areas that need strengthening in order to avoid potential data quality problems and root out those that arise.

Processes and Procedures

Steps in Data Flow Mapping:

- Start by outlining the current project framework for service delivery. Include a review of key project implementation processes in order to lay out the key data management elements.
- Identify all stages at which important program data are sourced; note when documents and data are received.
- List all essential data collection, collation, and analysis processes, and the tools used and the people responsible for managing each stage.
- List all reporting processes that the project uses to disseminate data to stakeholders.
- Identify real and potential data quality problems at various stages of data collection. Ask:
- Are there tools available for data collection, and are they appropriate?
- Are data collected consistently?
- Are the responsible people properly trained on the tools for data collection?
- How are the data analyzed, reported, and used for decision making?
- Is data integrity maintained? Consider here data security and the integrity of respondents and data collectors.
- Brainstorm and identify solutions to address data quality problems at each stage of data collection

Example of data flow mapping tools can be in Annex 9.11.

Processes and Procedures

Standard Operating Procedure Data Breach and Data Quality

There are several Standard Operating Procedures (SOPs) that can be put in place to facilitate the governance of farmers' data in a harmonized and streamlined fashion. The most relevant are:

SOP on data quality: This procedure provides detailed guidance on ensuring the quality of the data uploaded to the Kenya United Agriculture Data Platform (KUADP. Data quality validation should be undertaken using a variety of methods depending on how the data is stored. The following should be undertaken at least monthly and covered in a step-by-step guide in the SOP:

- Checking for the completeness of any data set and reviewing if missing information can be obtained and entered onto a system
- Undertaking regular checks on service user and farmers' data through rolling programs of audit to check for completeness.
- Validation of data entries
- Checking any data output or report against the live system from whence it came to prove validity and accuracy
- "Sense-checking' any information produced and comparing to similar or previous data sets.

See Annex 9.12 for a guide on data quality processes.

SOP in case of a data breach: This procedure outlines step-by-step how to act in the event of a privacy and information security incident as soon as it is reported. A template for an SOP in case of a data breach can be found in Annex 9.13.

Monitoring Processes

Audit and monitoring/control processes must also be put in place. Monitoring must be understood as a continuous control of both process and method used to process and collect personal farmers' data in order to detect compliance risk issues. Monitoring processes should be designed to test for inconsistencies, duplication, errors, policy violations, missing approvals, and incomplete and low-quality data. Monitoring methodologies include sampling protocols that permit identification and review variations from an established standard.

Processes and Procedures

Audits, on the other hand, entail reviewing the ongoing monitoring process and verifying if it is effective in achieving the desired result. When it comes to high-risk compliance areas like the use of personal farmers' data, audit objectives are to (i) verify that data stewards are meeting their monitoring obligations; and (ii) validate that the process is achieving desired results. This includes confirming that controls are in place and functioning as intended or identifying weaknesses in the monitoring process that need to be addressed. An audit must be an independent and objective review, which means it should be done by people external to the entity being audited.

Best practices when it comes to audit and monitoring include:

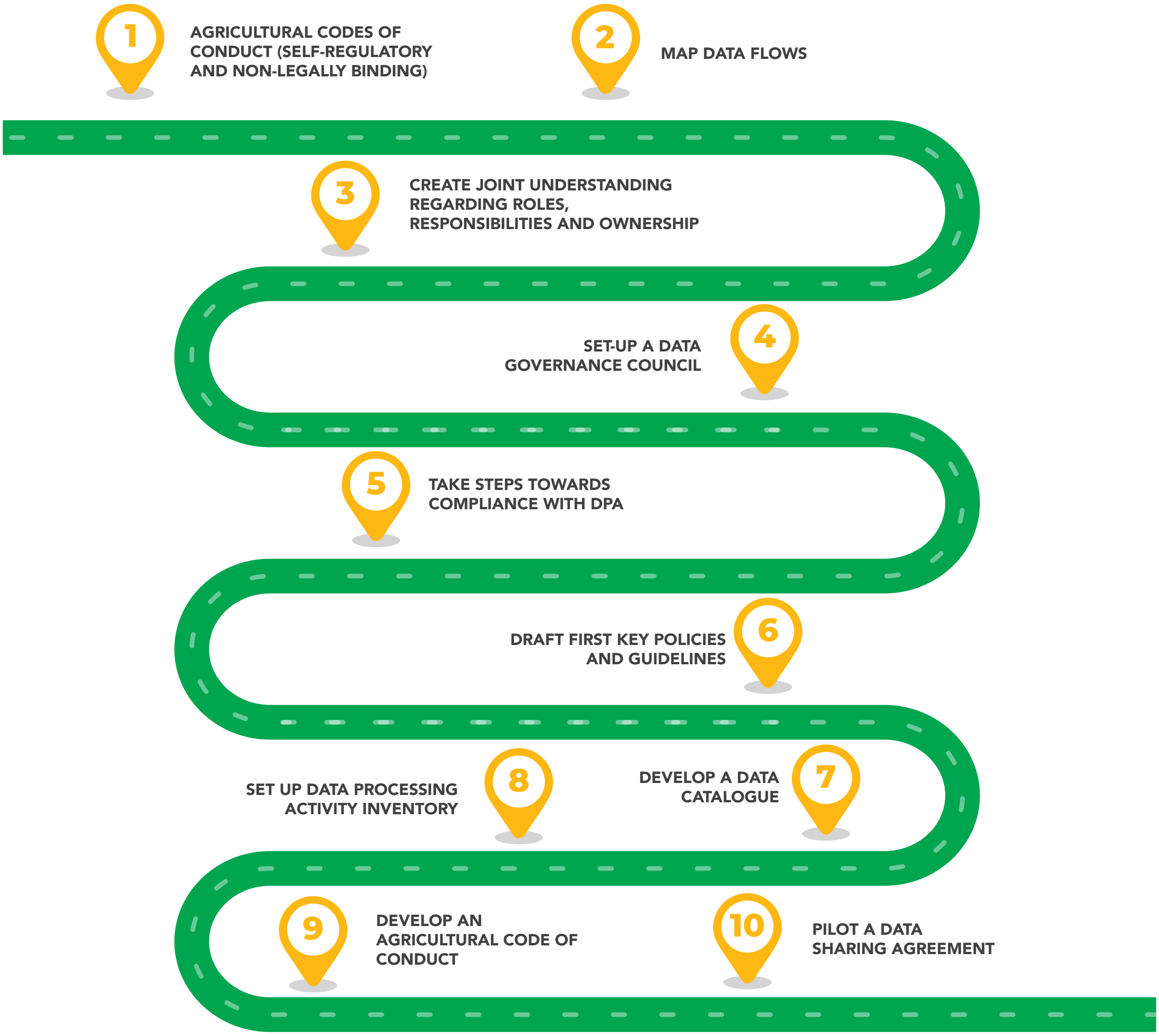
- Identify and make a list of compliance high-risk areas
- Create a compliance audit plan that will evaluate whether ongoing monitoring and auditing are adequately addressing compliance high-risk areas, giving priority to the areas of highest risk.
- Ensure responsible data stewards are engaged in assessing high-risk areas within their operations and have ranked them in terms of the level of risk, probability of risk exposure, and impact or damage that may result from that risk.
- Ensure that data stewards adequately develop and implement monitoring plans to address all risk areas
- Determine whether ongoing auditing has addressed the adequacy of the internal controls (e.g., policies and procedures) to reduce the likelihood that an unwanted, high-risk event will occur.
- Ensure that corrective action plans have been instituted for all deficiencies found within a risk area and verify that the corrective action works as intended.
- Include results of monitoring and auditing as regular agenda items in the Data Governance Council meetings
- Engage compliance experts to independently evaluate the effectiveness of a compliance program

7

ROAD MAP TOWARDS OPERATIONALIZING THE DATA GOVERNANCE FRAMEWORK

While Kenya's agriculture sector requires a comprehensive data governance framework, this roadmap focuses on the data governance for farmers' registration as an example that can be scaled to incorporate the other priority use-cases. Implementing the data governance framework will involve substantial change for all stakeholders operating in the data space of use case 1. The key to success will be collaboration between government (at national and county level) and private sector (at micro and meso level) in turning the framework into action. To facilitate the implementation of the data governance framework for farmers' registration data, **ten key steps** towards operationalization can be highlighted. They are presented in the following, build up on the status quo of farmers' registration data governance in Kenya, and offer concrete recommendations how to make the framework actionable.

Illustration 2: Agricultural Codes of Conduct Rationales


1
AGRICULTURAL CODES OF CONDUCT (SELF-REGULATORY AND NON-LEGALLY BINDING)
2
MAP DATA FLOWS
3
CREATE JOINT UNDERSTANDING REGARDING ROLES, RESPONSIBILITIES AND OWNERSHIP
4
SET-UP A DATA GOVERNANCE COUNCIL
5
TAKE STEPS TOWARDS COMPLIANCE WITH DPA
6
DRAFT FIRST KEY POLICIES AND GUIDELINES
7
DEVELOP A DATA CATALOGUE
8
SET UP DATA PROCESSING ACTIVITY INVENTORY
9
DEVELOP AN AGRICULTURAL CODE OF CONDUCT
10
PILOT A DATA SHARING AGREEMENT

7.1 DEVELOP A COMMON UNDERSTANDING OF SET OBJECTIVES

Step 1

The first important step in implementing the data governance framework for farmers' registration is engaging all relevant actors to align on the MoALFC high-level data use objectives for use case 1. Clearly documenting and communicating the data use objectives across stakeholders is a best practice that supports effective data governance and empowers actors who handle data efficiently and effectively. While the MoALFC Digitization Strategy establishes objectives regarding the collection and processing of farmers' data (for registration and impact monitoring), the understanding of the set objectives, namely what type of farmers' registration data is to be collected and for which purposes, is to date not completely agreed upon between the stakeholders involved. This discrepancy between the different understandings of the data to be collected for use case 1 and its objectives hinders interoperability, the further attribution of concrete roles and responsibilities, as well as the setup of the necessary data processes.

Recommendations

Organize a high-level leadership dialogue involving all relevant stakeholders to clearly communicate the objectives and relevant data types for use case 1 and also address questions that might exist in that context. This will help create a shared understanding of what types of farmers' registration data sets should be collected and for what purpose. Since the Digitization Strategy captures the MoALFC desired impacts, this document can be used as a baseline to align data objectives.

7.2 MAP DATA FLOWS

Step 2

Based on the reached common understanding with regards to the objectives for the collection of farmers' data under step 1, the next important step will be to understand the data's life cycle. This means mapping out the data flow of each type of data. More specifically, the following must be defined:

- → How the data will be collected (means, intervals, etc.) and by whom, into a master data source
- → Who will own the collected and processed data
- → Access to research data
- → Who will input the gathered data into the Kenya United Agriculture Data Platform (KUADP according to the set-out quality requirements
- → Which actors will be able to access the data once on the Kenya United Agriculture Data Platform (KUADP, and
- → Who will oversee data audits to spot false or inaccurate data

Recommendations

Fill in a data flow template to map out the life cycle of the identified data types. Define the responsibility (who collects, inputs, owns, access and audits the data?). Moreover, it would be useful to come up with a standardized nomenclature for domains and data elements for accurate interpretation and use.

7.3 CREATE JOINT UNDERSTANDING REGARDING ROLES, RESPONSIBILITIES, AND OWNERSHIP

Step 3

In pillar 1 of the data governance framework, the different roles and responsibilities are discussed, and suggestions are made with regards to the actors who might be able to fill the functions and oversee the tasks. As a fourth step towards the implementation of the framework, a common understanding and joint ownership must be developed regarding roles and responsibilities.

Recommendations

It is recommended to include the discussions around roles and responsibilities in the high-level leadership dialogue with an outcome statement in which all relevant stakeholders agree on the distributions of the roles, e.g., ATO as Steering Body and KALRO as host for the National Agriculture Data Platform.

Moreover, in view of the question on data ownership, the MoALFC will have to take a more significant lead since it will coordinate data collection in conjunction with the county governments. While the decision of who owns the data is a political one and must be taken at this level, when it comes to documenting data ownership a best practice would be to create a data sharing agreement that clearly outlines which entity owns the data uploaded to the National Agriculture Data Platform.

7.4 CREATE JOINT UNDERSTANDING REGARDING ROLES, RESPONSIBILITIES, AND OWNERSHIP

Step 4

To implement the framework successfully among and with the relevant stakeholders, the development of coordination mechanisms for effective liaison between national or county governments, development partners, institutions hosting and collecting the data, as well as farmers' representation is necessary.

Recommendations

MoALFC should take the lead in setting up a Data Governance Council.

7.5 TAKE STEPS TOWARDS COMPLIANCE WITH DPA

Step 5

As discussed, the DPA 2019 applies to the processing of personal data. It ensures that the processing of the personal data of a data subject is guided by the principles stated in the Act. Data collectors and processors of farmers' data related to use case 1 should adhere to these principles. Data controllers and data processors have a duty to 1) implement data protection principles in an effective manner; 2) integrate necessary safeguards into the processing, and 3) ensure that only personal data necessary for each specific purpose is processed.

Recommendations

As the first steps towards ensuring compliance with the DPA, data processors and controllers of farmers' data should register with the ODPC. For all the personal data already collected from farmers, consent must be sought. The consent template provided by ODPC could be adapted to the agricultural sector. Moreover, it is recommended to conduct a Data Protection Impact Assessment (DPIA) for the Kenya United Agriculture Data Platform (KUADP and use case 1, and conduct data protection awareness training as well as capacity development measures to sensitize staff handling farmers' data, e.g., about sound data privacy practices.

SMART FARMING PROGRAM
NPK
pH

7.6 DRAFT FIRST KEY POLICIES AND GUIDELINES

Step 6

While some actors like KALRO have already developed data policies, they still have to be created for the MoALFC and other involved actors to guide the appropriate use of farmers' data. Given that there are today already a number of policies from other countries available, not only could the Ministry build upon KALRO's work but also other reference documents.

Recommendations

Start with developing an internal data governance policy that can then guide the drafting of an external data policy and data protection and security guidelines.

7.7 DEVELOP DATA CATALOGUE

Step 7

During the interviews and consultations, it was noticed that among the staff of the different organizations and units handling personal data, unclarity existed about data quality requirements. Furthermore, only some stakeholders seem to keep a data catalogue of the farmers' data collected and processed (e.g., the ICT State Department of Cooperatives). Clear criteria and improved data quality are, however, essential for better decision-making, and the leveraging of the farmers' data gathered and utilized. The more high-quality data one has, the more confidence one can have in one's decisions. Good data decreases risk and can result in consistent improvements in results.

Recommendations

Create a joint Master data catalogue for the six data types of farmers' data across organizations building on the data catalogues already available. In addition, an aligned methodology determining which data types will receive priority and data governance resources (data handlers and stewards' time to document data processes, clean data, and create data outputs and reports).

7.8 SET UP DATA PROCESSING ACTIVITY INVENTORY

Step 8

Currently, data processing activities are not or at least not comprehensively enough documented (Agricultural Statistics Unit of MoALFC has some documented processes). Documentation of the processing activities is important in making the information about how personal farmers' data is used available on request, for example, for an investigation by the Office of the Data Protection Commissioner. As a key element of the accountability principle under the DPA, inventorying data processing activities helps ensure (and demonstrate) compliance with the data protection law. In addition, the inventory can help respond to access requests – knowing what personal data is held and where it is to be found allows for efficiency in handling requests from farmers for access to their personal information.

Recommendations

Document a data processing inventory by creating a cross-organizational inventory for use case 1.

7.9 DEVELOP DATA CATALOGUE

Step 9

To engage all stakeholders, especially farmers, into solutions around data sharing questions related to use case 1, Agricultural Codes of Conducts provide a great way to outline how farm data can be governed transparently and inclusively. As not all data flows on use case 1 are governed by the DPA, the different actors in the value chains have to protect themselves from the risks of data sharing. Codes of Conduct can foster mutual trust and transparency.

Recommendations

Through a multi-stakeholder approach, engage agricultural stakeholders, first and foremost farmers, in developing Kenyan Agricultural Codes of Conduct.

7.10 PILOT A DATA SHARING AGREEMENT

Step 10

As mentioned previously, data-sharing agreements are legal contracts between two or more organizations about how to share data. It will define what data is being shared and for how long, and any restrictions on its use. The agreements can be business-to-business (B2B) or business-to-government (B2G). In the context of the Kenya United Agriculture Data Platform (KUADP, which shall be hosted by KALRO, especially B2G data sharing agreements will be essential.

Recommendations

Build upon KALRO's work and experience with data sharing and pilot a first agreement for the sharing of farmers' data in the context of use case 1 and for the Kenya United Agriculture Data Platform (KUADP.

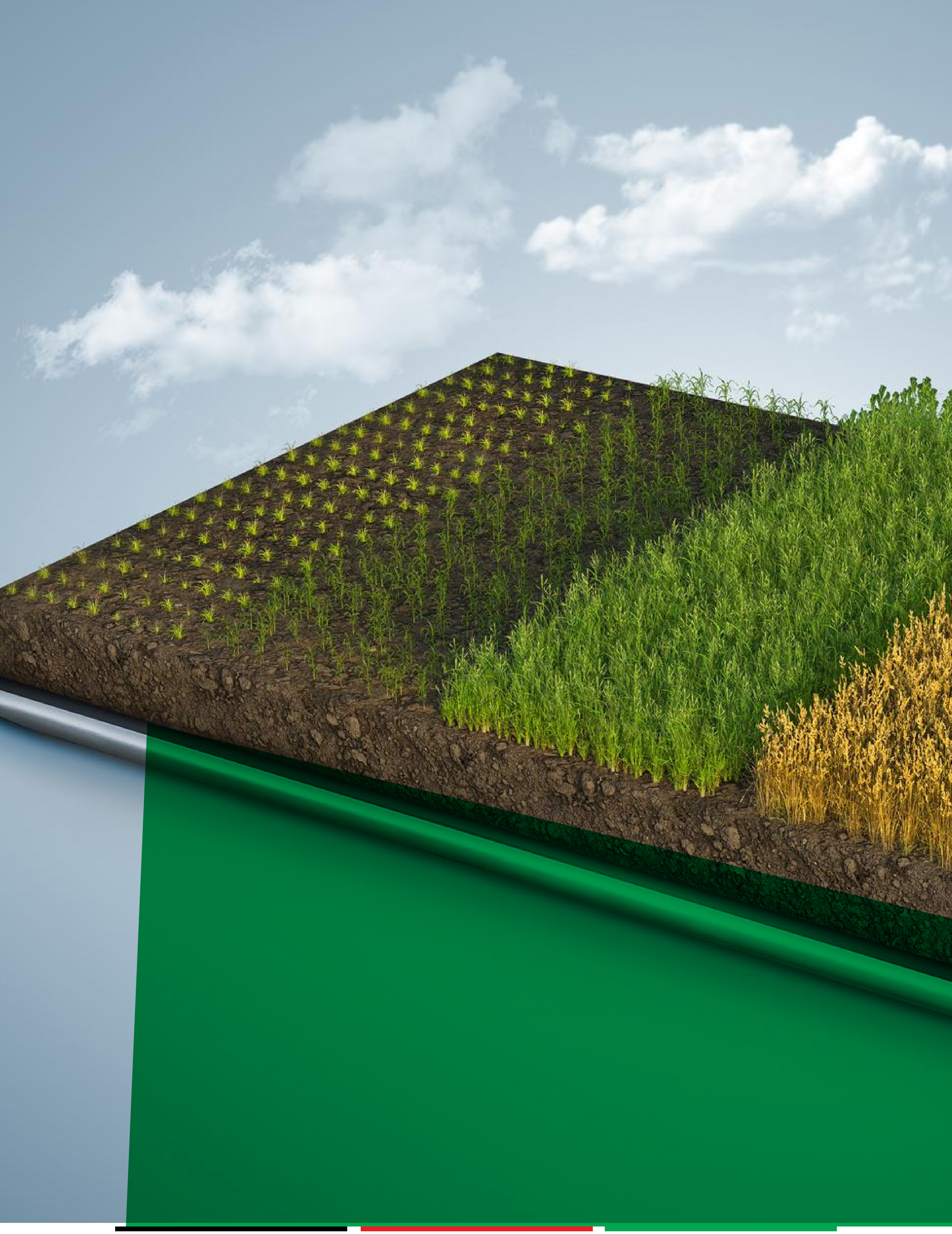
8

CONCLUSION

It is evident that the expansion of digital technologies has the potential to increase productivity, sustainability, and resilience of the agricultural sector and improve farmers' income and livelihood in Kenya. Nevertheless, a sound data governance framework – or the lack thereof – for agricultural data in many cases affects farmers' trust in digital technologies, or in many cases, the lack of their ability to harness the benefits of digital agriculture. More specifically, there are concerns about who controls access to data, and sharing of data generated on and about farms, and how the value created from that data is distributed. Concerns have also been raised about how agricultural data governance may affect the supply of digital services to farmers, with issues that may arise from lock-in effects, difficulties in discovering and using agricultural data, or cross-border restrictions of data flows.

The role of the Government in enhancing the institutional arrangements for the collection, discoverability, and usability of public and private agricultural data to support digital innovation of agro-food systems and better inform agricultural policies and services for farmers is essential. Government agencies collect, process, and hold a large amount of agricultural data that is of interest to various stakeholders such as researchers and the private sector, and farmers themselves. Consequently, there is a great need to leverage digital technologies to facilitate access to this data, particularly through open data arrangements. But there are also challenges related to having open access to data, mainly around privacy, data protection and security of farmers' data, exposure of commercially sensitive information, and fear of compliance oversight by other government agencies.

Understanding the importance of data and the great role that digital solutions play in agriculture, the Government of Kenya (GoK) has formulated the Agricultural Sector Transformation and Growth Strategy (ASTGS). The Ministry of Agriculture, Livestock, Fisheries, and Cooperatives (MoALFC) supports this strategy through the implementation of nine flagships. The Agricultural Transformation Office (ATO) is leading the efforts for the implementation of flagship 8 titled "Research, Innovation and Data," which is designed to "strengthen research and innovation and launch priority digital and data use cases to drive better decision-making and performance management." The MoALFC has identified seven priority use cases aligned with the primary ASTGS outcomes in its strategic document "Digitization and Coordination of Kenya's Agricultural Sector Data."



What has been observed with regards to all the identified use cases (1-6) is that different stakeholders, including the MoALFC, farmers, private sector, and researchers, have an interest in the same agricultural datasets, along with competing and/or complementary views on access, use and extracting value from them. Therefore, it will beessential to consider all stakeholders' concerns. The perspectives of farmers and a range of stakeholders have to be carefully understood when implementing the data governance framework for use case 1. Once the framework has been successfully piloted, lessons learnt and best practices can be gathered and used to further scale the framework to encompass the 2-6 use cases and related actors.

9

ANNEXES

9.1 EXAMPLES DATA GOVERNANCE POLICY

Many organizations have to date, already developed Data Governance Policies. The following provides a selection outlining the different approaches and structures that can be used:

- → Data Governance Policy King's College London
- → Data Governance Policy in the health sector
- → University of Technology UTS Data Governance Policy

9.2 HOWTO WRITE AN (OPEN) DATA POLICY

The Open Data Institute provides a guide with clear steps to pursue when developing an open data policy.

9.3 EXAMPLE DATA PROTECTION AND SECURITY GUIDELINES

- → Impact Initiative Data Protection Guidelines
- → OECD Privacy Guidelines
- → Samples of Data Security Policies

9.4 DATA RETENTION POLICY TEMPLATE

COMPANY NAME
Street Address
City, State, and Zip
webaddress.com

VERSION 0.0.0 **DD/MM/YYYY**

VERSION HISTORY

Version	Approved by	Revision date	Description of change	Author

Prepared by		Title		Date	
Approved by		Title		Date	

TABLE OF CONTENTS

PURPOSE OF THE POLICY

WHO IS AFFECTED BY THIS POLICY

KEY TERMS

TERM	DEFINITION

APPLICABLE LEGAL AND BUSINESS REQUIREMENTS

PROCEDURES FOR ENSURING DATA IS PROPERLY RETAINED

PROCEDURES FOR ENSURING DATA IS PROPERLY DESTROYED

APPLICABLE LEGAL AND BUSINESS REQUIREMENTS

PROCEDURES FOR ENSURING DATA IS PROPERLY ARCHIVED

EXCEPTION PROCESS

HOW TO RESPOND TO DISCOVERY, LEGAL, AND AUDIT REQUESTS

RESPONSIBILITIES OF THOSE INVOLVED IN DATA RETENTION

DUTIES OF THE DATA RETENTION TEAM (If applicable)

DEFINITION OF TEMPORARY RECORDS

DEFINITION OF WHAT DOCUMENTS CAN BE IMMEDIATELY DELETED

For more data retention policy templates, click here.

Other relevant links with guidelines on developing a data retention policy:

- → Top Tips for Data Retention under the GDPR
- → Data Retention Policy 101: Best Practices, Examples and More
- → Data Retention Policy: What it is and how to create one

9.5 EXAMPLE DATA PROTECTION IMPACT ASSESSMENT

The Office of the Data Protection Commissioner (ODPC) has developed guidelines and templates on DPIA (how to identify risks arising from the processing of personal data and how to minimize these risks).

The following template is an example of how to record a DPIA process and outcome. The template should be filled out at the start of any major activity involving the use of personal data or if significant changes are made to an existing process encompassing personal data. The final outcomes should be integrated back into the activity plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link other documents, such as a project proposal. Summarize why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and the delete data? What is the source of the data? Will you be sharing the data with anyone? You might find it useful to refer to a flow diagram or any other way of describing data flows. What types of processing identified are likely to involve high risks?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any has been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organization? Do you need to ask your processors to assist? Do you plan to consult information security experts or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe the source of risk and the nature of potential impact on individuals. Include associated compliance and corporate risks if necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible, or probable	*Minimal, significant, or severe*	*Low, medium, or high*

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.				
Risk	**Options to reduce or eliminate risk**	**Effect of risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	*Low medium high*	*Yes/no*

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		*Integrate actions back into the project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any high residual risk, consult the local DP Authority before going ahead*
DPO advice provided:		*DPO should advise on compliance, step 6 measures, and whether processing can proceed*

Summary of DPO advice:

DPO advice accepted or overruled by:	**If your decision departs from individuals' views, you must explain your reasons**

Comments:

Consultation responses reviewed by:	**DPO advice accepted or overruled by:**

Comments:

This DPIA will be kept under review by:	**The DPO should also review ongoing compliance with DPIA**

Source: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

9.6 AGRICULTURAL CODE OF CONDUCT DEVELOPMENT TOOL

GODAN has created a tool to allow selecting of Clauses that might be relevant, letting one easily produce a printable and savable Code of Conduct: GODAN Code of Conduct KIT

9.7 INFORMED CONSENT TEMPLATES AND GUIDES

- Guidance and template on informed consent by the Office of the Data Protection Commissioner (ODPC)
- GDPR consent guidance
- How to seek free, prior and informed consent (FPIC) Examples from IFAD investment projects
- Berkley informed consent form and guidelines
- Berkley Instructions for signed versus unsigned informed consent

9.8 EXAMPLE DATA SHARING AGREEMENT

The following data sharing template was developed by KALRO and can serve as a good example of how to formulate such a legal agreement between two organizations:

[Logo organization A] [Logo organization B]

PREAMBLE

This MEMORANDUM of UNDERSTANDING (hereinafter referred to as "MOU" is made on dd/mm/yyyy between:

[Organization A] located on [street], [city], Kenya (hereinafter referred to as "A" which expression shall, where the context admits, include its successors and assigns) of the first part

AND

[Organization B] located on [street], [city], Kenya

AND

[Organization A] and [Organization B] are individually referred to herein as a “Party” and collectively as the “Parties”,

RECITALS

WHEREAS [Organization A] [description of organization A + mission]

WHEREAS [Organization B] [description of organization B + mission]

WHEREAS [Organization A] and [Organization B] [description of joint goal]

WHEREAS, this MOU is based on principles of trust, equality, and mutual benefits;

NOW, THEREFORE, the Parties have come to the following understanding:

OBJECTIVE

The objective of this MOU will be to establish a framework to facilitate cooperation between the two institutions on …

ARTICLES OF OBLIGATIONS

In order to collaborate effectively, the Parties agree to the following obligations:

ARTICLE 1: OBLIGATIONS OF A

A will facilitate B to access its content in agricultural and livestock sectors during the execution of specific Scope of Works (SOWs)

A will facilitate and support B in establishing collaboration with other A partners focusing on agricultural and livestock data and other relevant technology dissemination during the execution of specific Scope of Works (SOWs)

ARTICLE 2: OBLIGATIONS OF B

B will work within the established and/or agreed frameworks under A either directly or through other A partners.

B will identify opportunities for collaboration with A that will advance the Parties' shared interests.

ARTICLE 3: JOINT OBLIGATIONS

The Parties agree to:

Take all the necessary technical and organizational measures in the collection and sharing of farmers' personal data and be compliant with the Kenya Data Protection Act 2019

3.2 Other obligations…

ARTICLE 4: DURATION

This MOU shall become effective immediately upon signature by the appropriate authorized representatives of each of the two institutions and shall remain valid for a period of [months/years] subject to review and/or termination as may be necessary by either party.

This MOU may be renewed by a mutually written agreement of the parties hereto, executed at least [months/years] prior to the expiration of the initial term.

ARTICLE 5: TERMINATION

Either Party may terminate the MOU at any time upon notice of its decision at least three (3) months in advance, without the right to any compensation for the other Party. If, at the moment of the unilateral termination, specific tasks are pending, they will continue until the end of the said specific task.

Upon termination, any gains or losses in the pursuance of the provisions of this MOU shall be shared on mutually agreed ratios; failing such agreement, the same shall be shared equally between the parties.

Termination of Cause: Each Party shall have the right to terminate this Agreement or any SOW immediately upon a written notice in the event (a) the other Party is in material breach of this Agreement or such SOW, and such breach is not cured within thirty (30) days after receipt of written notice of the breach, or (b) if the other Party makes a general assignment for the benefit of creditors, or files a voluntary petition in bankruptcy, or if an involuntary petition in bankruptcy or similar proceeding is filed against such other Party and is not dismissed within ninety (90) days.

Survival: Articles 6, 11, and 12 shall survive the termination of this Agreement for any reason, together with any accrued but unpaid payment obligations and any other provisions which by their plain meaning are intended to survive.

ARTICLE 6: CONFIDENTIALITY

During the course of this MOU, either party may acquire confidential information or trade secrets of the other. Confidential information of a party means all information of whatever description, whether in permanently recorded form or not, and whether or not belonging to a third party, which by its nature is confidential or which the party identifies as confidential to itself.

It does not include information that is:

Independently created or rightfully known by, or in the possession or control of, the other party and not subject to any obligation of confidentiality on the other party;

In the public domain (otherwise than as a result of a breach of this agreement);

Required to be disclosed by law; was or is independently developed by the Receiving Party without use or reference to any information obtained from the Disclosing, or any Party acting on behalf of the Disclosing Party, as demonstrated by the Disclosing Party's written records.

The Parties, together with their representatives, agents, and personnel, shall keep confidential anything which the other designates as, or which might reasonably be expected to be, confidential, unless otherwise required by a competent authority.

ARTICLE 7: NON-EXCLUSIVITY

Unless otherwise agreed, this MOU is a non-exclusive agreement, and both Parties are free to carry out other projects of any nature whatsoever with third parties.

ARTICLE 8: GOVERNING LAW

The Parties agree that the laws of Kenya shall apply to this MOU.

ARTICLE 9: SETTLEMENT OF DISPUTES

9.1 Amicable Settlement

The parties undertake for themselves, their agents, and/or servants to observe all established rules and regulations and to make further rules and regulations to govern the use of facilities in the conduct of any or all of the functions of this MOU. The parties shall use their best efforts to amicably settle all disputes arising from or in connection with this MOU or interpretation hereof.

9.2 Right of Arbitration

Any dispute between the parties as to matters arising pursuant to this MOU which cannot be settled amicably within THIRTY (30) DAYS after receipt by one party of the other party's request for such amicable settlement may be submitted to an Arbitrator mutually agreed upon by the parties for a decision in accordance with the provisions of the Arbitration laws of Kenya.

ARTICLE 10: FORCE MAJEURE

Neither party shall be liable in damages or have the right to terminate this MOU, for any delay or default in performing hereunder, if such delay or default is caused by conditions beyond its control, including, but not limited to Acts of God, Government restrictions (including the denial or cancellation of any operational or other necessary licenses), wars, insurrections and/or any other cause beyond the reasonable control of the party whose performance is affected.

ARTICLE 11: INDEMNITY

The parties always agree to keep each other fully and properly indemnified against all damages to or losses of any of their respective facilities resulting from negligent acts of omission or commission of their respective agents and/or servants.

ARTICLE 12: INTELLECTUAL PROPERTY AND CO-AUTHORSHIP

A shall retain ownership of all intellectual property rights, title, and interest XX that is not subject to this Agreement.

Organization's IP

The Parties acknowledge and agree that all rights in and to any Intellectual Property created or arising from the content creation and design other than the Intellectual Property described in 12.1 & 12.2 shall be owned jointly by the parties, and the revenue made from commercializing the co-created content shall be shared equally.

Other IP agreements on research, e.g., Parties shall periodically review the results of research projects to determine if any research findings, including processes and methods, constitute patentable technology.

Other IP agreements on the disclosure of proprietary information, e.g., Parties agree that prior to any disclosure of proprietary information by one party to the other concerning a specific aspect of this collaboration; the disclosing party may require the other to execute a confidentiality agreement in respect of the information.

Other IP agreements on publications, e.g., Material for publication or presentation from the joint collaborative activities, shall be submitted for clearance to A to ensure that no patentable discoveries are published prior to protection by patents.

ARTICLE 13: RELATIONSHIP BETWEEN PARTIES

Nothing contained herein shall be construed as establishing a relationship of agent and principal or master and servant as between the parties. Each party shall have full control of its operations and undertakings and shall be responsible for activities and duties carried by and on its behalf.

ARTICLE 14: INSURANCE

In carrying out the functions of this MOU, each party will insure its own employees and ensure that all adequate safety precautions are in place.

ARTICLE 15: NOTICES

Any notification, request, or consent required or permitted to be given or made pursuant to this MOU shall be in writing. Any such notification, request, or consent shall be deemed to have been given or made when delivered in person to the authorized representative at the Head Office of the party to whom the communication is addressed or when sent by registered mail, fax, or E-mail (signed attachments) to such party at the following address:

For:

Head Office Representative

Organization A

P.O. Box:

Fax:

E-mail:

For:

Head Office Representative

Organization B

P.O. Box:

Fax:

E-mail:

PROVIDED THAT a party may change its address, e-mail, and fax number for communication hereunder by notifying the other party of such change pursuant to this clause. Notice shall be deemed to have been received one day after dispatch by electronic means and five days after dispatch by ordinary post.

ARTICLE 16: AUTHORIZED REPRESENTATIVE

Any action required or permitted to be taken, and any document required or permitted to be executed under this MOU may be taken or executed:

on behalf of A by the [Head of Office representative] or any other Officer appointed in writing by the [Head of Office representative] to carry out that function on behalf of organization A.

ORAGNIZATION A	ORGANIZATION B

In witness thereof, the representatives of the agreeing Parties are duly authorized sign this MOU on the date indicated below:

By: ____________________	By: ______________________
(Signature)	(Signature)
Name: _________________	Name: ____________________
Title: _________________	Title: ____________________
Date: ________________	Date: ___________________
In the presence of (….)	In the presence of (….)
Signature: _____________	Signature: _______________
Name: ________________	Name: __________________
Date: ________________	Date: _________________

Further relevant links:

- → Data sharing agreement guide from Chatham House
- → Data sharing agreement template and support pack from CGIAR
- → Outputs management plans from Welcome foundation
- → Data sharing checklist from the UK Information Commissioner
- → https://datasharing.chathamhouse.org/guide/principles/agreements/

9.9 DATA CATALOGUE TEMPLATE

Attribute	***Description***
ID	Unique identifier for the dataset
Title	The name of the data asset
Description	A description of the data asset
Purpose	Why was the data collected or produced?
Data creator	Who created the data?
Data manager/owner	Who manages the data?
Subject/keywords	What subjects/topics does this dataset cover? This will help in discovery for users searching for this data. It is recommended to use a controlled vocabulary for this attribute (and others where possible) to improve future search and data linking potential, e.g., finding related datasets.
Location	Where is the data located or stored?
Creation date	When was the data created?
Update frequency	How often is the data updated?
Type	What type of data is it? Text, numbers, statistics, images, a database?

Attribute	***Description***
Format	What format is the data in? E.g., MS Excel, CSV, JPEG, SQL DB
Rights and restrictions	What are the access and usage rights and restrictions? If you are publishing the data, what can users do with the data? Include a link to the relevant license for the use of the data (e.g., Creative Commons or a bespoke license)

9.10 TEMPLATES DATA LICENSE REGISTER

→ Agricultural license Government of India

→ Australian Business License and Information Service

→ Publisher's Guide to Open Data Licensing – The ODI

9.11 DATA FLOW MAPPING TOOLS

Data Mapping Tools help map data to and from various data sources. They automate the mapping process or assist in mapping data seamlessly without much effort. There are open-source Data Mapping Tools or purchasable Data Mapping Tools. Some of the most commonly used tools are listed below:

→ Creately Data Flow Templates

→ Edraw Free Data Flow Templates

→ MURAL Data Flow Diagram Template

9.12 SOP GUIDE DATA QUALITY

Pactworld has developed a Field Guide for Data Quality Management, with an Excel-based Routine Data Quality Assessment (RDQA) Tool, including instructions on how to use it. The Guide also provides a Data Quality Management (DQM) SOP template that can be customized to individual projects.the most commonly used tools are listed below:

9.13 SOP DATA BREACH

STANDARD OPERATING PROCEDURE (SOP) DATA BREACH

1. PROCEDURE

1.01 Definition: What is a Breach?

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Such incidents may be caused by:

- Accidental loss
- Theft
- Human error, e.g., e-mails containing personal data sent to the wrong person
- Equipment failure
- Damage, e.g., fire, flood
- Malicious activity, e.g., hacking

If a data security breach occurs, the [organization] will respond to and manage the breach effectively using a seven-part process.

1. Reporting a Breach

2. Containment and Recovery

3. Assessing the Risks

4. Notification of Breaches

5. Evaluation and Response

6. Communication Plan

7. Review

1. Reporting a Breach

The DPA (2019) requires the [organization] to report breaches to the Office of the Data Protection Commissioner (ODPC) within 72 hours of it being discovered.

It is therefore critical that once any member of staff or authorized third party of the [organization] that has knowledge of a breach must contact the ODPC immediately.

Delays in reporting to the ODPC must be accompanied by an explanation of reasons for the delay. Contact details are:

CA Centre

Waiyaki Way

P.O Box 30920-00100

G.P.O Nairobi

info@odpc.go.ke

0796954269

All known details should be included in the initial reporting of the incident.

The immediate response will be to establish the nature of the breach and the data involved, e.g., is it personal? How many individuals may be affected? This will determine which Data Stewards of the [organization] must be notified.

The [organization's] Data Protection Officer (DPO) must report all breaches to the [organization's] management team.

Confirmation of a breach having occurred will activate an official record being made of the circumstances leading to the breach, managing the data loss, individuals involved and evaluation/recommendations.

2. Containment and Recovery

Once details of the breach are known, the DPO will liaise with relevant personnel to contain the effect of the breach. This may include personnel from ICT (data handlers, data stewards), Human Resources, Management Team, and on some occasions, external suppliers.

The DPO and the data stewards will agree on what action must be taken to limit the damage caused by the breach and, if possible, restore any lost data, e.g., backup tapes. Priority actions may include password changes, disabling swipe access to secure areas within the buildings, or searching for lost equipment.

3. Assessing the Risks

Once the breach has been contained, the DPO and data stewards will assess risks associated with the loss of the data.

Considerations will be given to the following points:

- Type of data, e.g., hardcopy, electronic, personal data, sensitive data
- Nature of the loss, e.g., theft, damage
- Has the data been encrypted?
- What information does the data tell an unauthorized party who may now have access?
- How many individuals are potentially affected by this loss?
- What category of individuals are affected, e.g., farmers?
- What threat may be posed to these individuals, e.g., financial loss, personal safety?

4. Notification of Breaches

Where data loss has been confirmed, the [organization] is obliged to notify all parties affected by the breach.

Notifying the individuals

The DPO and data stewards will establish the identities of individuals whose personal data has been compromised and agree on the correspondence to be sent to each subject.

The correspondence should include:

- how and when the breach occurred
- what data is involved
- actions taken by the [organization]
- advice in relation to what steps the individual may need to take to protect themselves in light of their data being compromised, e.g., changing a password has the ODPC been informed?

- contact name, website link if they need further information concerning the incident

Notifying the ODPC

The ODPC must be notified of all breaches where large numbers of individuals are involved or where the consequences are serious, within 72 hours – the DPO will be responsible for this correspondence.

When notifying the ODPC, the information should include, at a minimum:

- nature of the personal data breach, including, where possible, the categories and an approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned
- name and contact details of the DPO or other contact points where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The ODPC will not normally inform the media of a breach; however, they may advise the [organization] to inform the media of the breach.

Notifying the Media

Should the ODPC advise that the media has been informed of the data breach, the DPO will liaise with the Management Team of the [organization] to agree on a statement which will be released to the press via the [organization's] Communications department, containing all relevant information pertaining to the incident.

5. Evaluation and Response

While it is critical to contain and assess the risks of a breach, the [organization] must evaluate events leading to the breach and the effectiveness of its response to it. While carrying out an evaluation, the DPO will convene with department specialists, a member of CMT, and if necessary, seek advice from the ODPC regarding what measures the [organization] should and can take to avoid a breach of a similar nature in the future.

Considerations should be given to the following:

- Was the breach a result of inadequate policies or procedures?
- Was the breach a result of inappropriate training?
- Where are documents stored?
- Who has access rights to what data?
- Has this breach identified potential weaknesses in other areas?
- Security of electronic information assets

5.01 ODPC Response

The ODPC will evaluate the data breach and carry out their own investigation into the surrounding circumstances, the nature and seriousness of the breach, and the adequacy of any remedial action taken by the [organization] will be assessed, and a course of action determined.

The ODPC may:

- Record the breach and take no further action, or
- Investigate the circumstances of the breach and any remedial action, which could lead to:
- no further action;
- a requirement on the data controller to undertake a course of action

to prevent further breaches;

- formal enforcement action turning such a requirement into a legal
- obligation; or
- where there is evidence of a serious breach of the DPA, whether deliberate or negligent, the serving of a monetary penalty notice requiring the [organization] to pay a monetary penalty of an amount determined by the Commissioner.

Recommended changes to systems, policies, and procedures will be documented and implemented as soon as possible thereafter.

6. Communication Plan

This procedure will be communicated to all staff via the [organization's] Intranet.

7. Review

This procedure will be reviewed (and amended if required) biannually or sooner to reflect changes in legislation or circumstance.

REPUBLIC OF KENYA

MINISTRY OF AGRICULTURE,
LIVESTOCK, FISHERIES AND CO-OPERATIVES

german
cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

DIGITAL
TRANSFORMATION
CENTER KENYA

KENYA
VISION 2030

THE BIG 4
EMPOWERING THE NATION

ASTGS 2019 2029
AGRICULTURAL SECTOR TRANSFORMATION AND GROWTH STRATEGY
Towards Sustainable Agricultural Transformation and Food Security In Kenya