MALAYSIA AGRICULTURE DATA SHARING CODE OF PRACTICE

29 October 2021

Table of Contents

Section 1: Introduction

1.1 About the Code of Practice

Agriculture is viewed as an important economic sector in Malaysia and is a major contributor to the gross domestic product (GDP) of the country. Some of the major agriculture subsectors in Malaysia include oil palm, livestock, fishing, forestry and logging, and rubber.

The agriculture sector provides employment for more than 1.5 million people in Malaysia[1]. As such, this sector has the potential to accelerate economic growth through job creation as well as generate sustainable income for farmers. In the Twelfth Malaysian Plan (2021–2025), modernisation and transformation of the agriculture sector is given priority, with a focus on accelerating the adoption of smart farming. This will help improve food security, increase crop productivity, increase farm profitability, strengthen the agri-food supply chain, as well as enhance related support and delivery services for all stakeholders.

Given the importance of the sector, the Malaysian agriculture sector has seen a gradual adoption of technology such as Internet of Things (IoT), data analytics, GPS, cloud computing, drone, robotics, and automation. This is in line with the need to increase production and profit in the sector and to also attract a younger generation of farmers to help with what is perceived to be an aging workforce. With the shift towards more digitisation in the agriculture sector, data takes centre stage. With an increase in digital farming and exchange of data, it becomes important that data sharing along the agriculture value chain is conducted in a fair and transparent manner.

Agriculture data is very diverse and covers data such as livestock and fish data, land and agronomic data, climate data, machine data, financial data, and compliance data. Subsets of these data can be viewed as sensitive or confidential information by stakeholders in the agriculture value chain which makes it important that necessary safeguards are put in place to protect it. To promote a safe and open data sharing culture among all stakeholders of the agriculture value chain, the potential benefits as well as risks and mitigations should be made clear. This should be well documented and constructed in a contractual form to remove ambiguity and gain trust.

It is therefore crucial to define key principles on data rights, be it proprietary or similar rights, access rights and/or data reuse rights. Transparency and responsibility are key to gaining trust and overcoming the fear of sharing data. If such principles are established and followed, then it will be possible to construct business models that benefit all stakeholders involved. Malaysia's Agriculture Data Sharing Code of Practice intends to provide general guidelines when it comes to sharing of agricultural data in the agriculture value chain.

[1] DOSM (2020). *Selected Agricultural Indicators, Malaysia, 2020*. Retrieved from https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=72&bul_id=RXVKUVJ5TitHM0cwYWxlOHcxU3dKdz09&menu_id=Z0VTZGU1UHBUT1VJMFlpaXRRR0xpdz09

1.2 Objectives of the Code of Practice

a) The objective of this code of practice is to facilitate an open and safe data sharing environment in the agriculture sector by ensuring that all stakeholders in the agriculture value chain have confidence in how their data is collected, used, and shared.

b) The code of practice aims to establish principles for the collection and usage of agriculture data around the following key areas: -

   i. Increase awareness around the collection, use, and sharing of agriculture data.

   ii. Improve transparency, clarity, and honesty in the way agriculture data is collected, used, and shared.

   iii. Ensure fair and equitable collection, use, and sharing of agriculture data.

   iv. Build trust and confidence in the way agriculture data is collected, used, and shared.

   v. Ensure adaptability of the code of practice to encourage agriculture stakeholders to establish appropriate practices around agriculture data collection, use, and sharing.

c) This code of practice outlines broad suggestions and recommendations for stakeholders in the agriculture value chain to have good data sharing practices.

d) Adherence to this code of practice is on a voluntary basis, although it is highly encouraged for any agriculture stakeholder that collects, uses, and shares farm data to adopt the data sharing principles outlined in the code of practice.

1.3 Definitions

a) The code of practice covers three categories of data namely: -

   i. Public Data – Data from any source which relates to agriculture or stakeholders in the agriculture value chain, that can be freely used, reused, and redistributed by anyone with no existing local, national, or international legal restrictions on access or usage.

   ii. Farm Data – Data created by a farmer, or a service provider in the course of providing a service to a farmer (a farmer refers to an individual, partnership, or business which operates a farm).

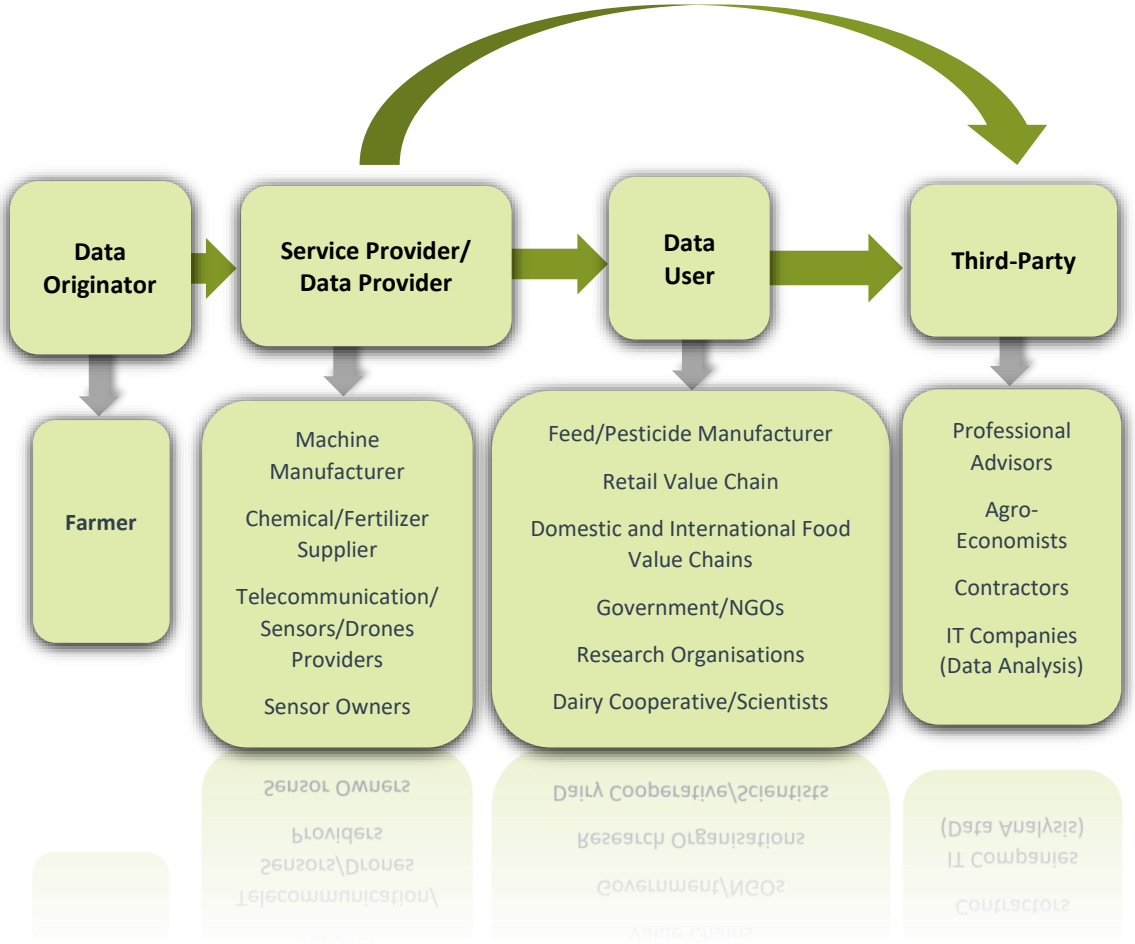
   iii. Private Data – Data that is identifiable to an individual farmer or their business.

b) The code of practice aims to cover the agriculture value chain which consists of stakeholders such as farmers, feed/pesticide manufacturers, sensor owners, the retail sector, government/NGOs, research organisations, and many others. The role of the stakeholders in the agriculture value chain varies depending on the activities performed and hence fall into the category of either Service Provider/Data Providers, Data Users or Third-Party organisations, with farmers as the Data Originators in a typical scenario.

c) Data sharing refers to the disclosure of data from one or more organisations to another organisation(s), or the sharing of data between different parts of an organisation.

1.4 A Typical Agriculture Value Chain

Depicted below is a representation of a typical agriculture value chain and the various categorisation of each stakeholder based on their roles: -



Section 2: Code of Practice

2.1 Data Ownership

a) A data originator is termed as any party who produces data within the agriculture value chain. Therefore, ownership of this data including the right to determine who can access and use the data must belong to the data originator. An example for this would be farm data that is produced by a farmer. In this scenario, the farmer should have the rights to own and determine the usage of this farm data.

b) There are various levels of data ownership in an agriculture value chain due to the various means of data collection. It is therefore important to have a clear contract to be established between all parties of the agriculture value chain such as the data originator, data provider, data user or third-party to ensure that there is a clear understanding and agreement on data ownership and usage among all contracting parties.

c) The contract must clearly address the protection of sensitive information such as intellectual property information for all parties. As an example, if a fertiliser manufacturer has developed a particular mix of fertiliser that promotes healthy growth of vegetables through research and development performed by the fertiliser manufacturer, and if details around the mix of the fertiliser is shared with a farmer or a third-party like a research firm, the contract must clearly state how the fertiliser supplier's intellectual property will be protected by the farmer and the research firm.

d) The contract must clearly state that data should not be used, processed, or shared without the consent of the data originator.

e) Ownership of data must be clearly attributed to the data originator, allowing the originator to outline the access and use of their data.

f) Any contract that is created must utilise simple and easy to understand language in order to explain data-related attributes.

g) Areas that should clearly be stated in the contract include: -

   i. Terms and definitions.

   ii. Purpose of collecting, sharing, and processing the data.

   iii. Rights and obligations that the parties have related to the data.

   iv. IT platforms and processes around the storage and use of the data.

   v. Verification processes for the data originator.

Relevant Existing Act Referred

a) The Personal Data Protection Act 2010 (PDPA), in covering rights for personal data, provides the following provisions when it comes to data ownership: -

   i. A data user should not process personal data unless consent has been provided by the data owner.

   ii. A data user can process personal data from a data originator within the boundaries of a contractual agreement with the data originator.

2.2 Data Sharing (Access, Control and Portability)

a) The required approval or permission must be obtained from a data originator prior to any collection, access, storage, or usage of agriculture data. This can be outlined via a contractual agreement. As an example, if an agriculture company intends to collect and use farm data from a farmer, both parties should have a contract in place that clearly details the farmer's approval.

b) In the event the data originator wishes to remain anonymous, data must be anonymised. Otherwise, the contract should specify the conditions when a data originator needs to be identifiable. An example here would be in a scenario of being able to trace data back to a particular farm for example due to the needs to showcase sustainable farming practices. In such a scenario, it may be required for the data user like an agriculture company to be able to share data around farm details such as location and farming practices to a third-party such as an international trade organization. Therefore, in this scenario, the agriculture company should specify the conditions in the contract with the farmer on which data will not be anonymised and the reasons for it.

c) If there is a need for data to be shared with a third-party, the required approval or permission must be obtained from the data originator and the data shared must be in an anonymised or aggregated form. If there is to be any deviation to the above, it must be specified in the contract to be agreed with the data originator.

d) A data provider must ensure that access to any data that has been obtained from a data originator is properly audited and any changes made to the data is traceable. As an example, if a data provider like a sensor owner is storing data from a farm, the sensor owner should put measures in place to ensure that access and changes to the farm data is tracked and recorded. This can be done utilising IT solutions such as identity and access management software that can help with access control and audit.

e) A data provider should also ensure that data obtained from a data originator is also easily accessible to the data originator themselves. Any contract put in place must outline that the data originator will have the right to receive data that originated from them or is attributable to their operations. As an example, if a research organisation is collecting and storing farm data on a premise server or in a cloud solution, the farmer must be given the required credentials to access his/her farm data in those storage solutions.

f) In any event that there would be a need to restrict the data originator from sharing their data to other users, then this must be clearly addressed in the contract and agreed between the data originator and data provider. Ideally, data originators should not be restricted should they wish to use their data in other platforms or data storage facilities unless it is stated in the contract and agreed upon.

g) The contract must clearly outline how restricted access to information like machine data or sensitive data will be handled between stakeholders such as farmers and service providers. For example, if a machine manufacturer is providing access to a farmer to the machine manufacturers storage solution that may contain data from other farmers, it becomes important to specify what kind of access rights will be given to the farmer to ensure they are not able access the data of other farmers.

h) Having centralised data sharing platforms helps when trying to encourage data sharing within an agriculture value chain. Clarity must be provided to data originators and data users of the platform on which data is only to be viewed by data originators, which data can be shared within stakeholders of the value chain, and which data is considered open or public data.

Relevant Existing Acts Referred

a) The Personal Data Protection Act 2010 (PDPA), in covering rights for personal data, provides the following provisions when it comes to data sharing: -

    i. A data user should not process personal data unless consent has been provided by the data owner.

    ii. A data user will have to provide a formal written notice to a data owner should they wish to process personal data on behalf of the data owner which includes details on description of the personal data, purpose of collection and sharing of the personal data, information on the source of the personal data, rights of the data owner to be able to request access and to correct the personal data, the stakeholders that the data user will be sharing the personal data with and the boundaries of the sharing of this personal data.

    iii. A data owner should also be promptly notified by the data user whenever the data user first collects personal data, uses the personal data for reasons other than was agreed upon or discloses the personal data to a third-party.

    iv. A data owner will also have the authority to correct personal data where it is inaccurate or incomplete, outdated, or misleading and withdraw consent to process personal data.

b) The Computer Crimes Act (1997), provides the following provisions when it comes to data sharing: -

    i. It is a punishable offence if unauthorised access to any computer material is performed.

ii. It is a punishable offence if unauthorised modification of computer material is performed.

iii. It is a punishable offence if unauthorised access to any computer material is performed with the intention of further utilising the material obtained.

c) The Communications and Multimedia Act 1998 (CMA) mentions that interception and disclosure of communications or attempts to intercept and disclose to any other individual the contents of any communications are forbidden.

2.3 Data Trust (Privacy and Security)

a) When it comes to data trust, any contract that is put in place must clearly outline the responsibilities of a data user/data provider in terms of security and data confidentiality.

b) A data user or provider must always have good record keeping of data that is being utilised along the agriculture value chain and must always ensure that this information is accessible to the data originator.

c) A data user must also ensure to always protect data obtained from a data originator from being lost, stolen, hacked into, or altered by any party that are not authorised. It is recommended as a best practice for data users/data providers to appoint a data protection officer to ensure that a data originator's right is maintained. There must be the option to remove, destroy, or return all original data upon a data originator's request at any point in time.

d) A communication process must be put in place to ensure that a data originator is promptly informed in the event of any breach or tampering of their data. As an example, if a data user such as a research organization that stores farm data in their servers experience a hacking attempt, then a prompt notification should be sent to the data originator informing of the breach. The turnaround time and manner of communication to the data originator of the breach must be outlined in the communication process.

e) Data users who store data from data originators must implement a data back-up and recovery regime that is appropriate for the scale, sensitivity, and timelines of the data stored. As an example, if a large palm oil company is storing large amounts of critical data from data originators such as farms or mills in on-premises servers, the palm oil company will need to ensure that data on the primary servers are backed up in secondary servers or in a secondary data centre. In the event the primary servers go down for any reason, data would still be accessible via the secondary servers.

f) Stored data must be encrypted and there should be access control mechanism at each data storage device or software, whereby proper registration and credentials are needed to access specific fields of data. Where possible and dependent on the scale and criticality of the data, it is recommended to engage with reputable data centres for the secure storage of data.

Relevant Existing Acts Referred

a) According to the Personal Data Protection Act 2010 (PDPA), a data user is required to take practical measures to protect personal data from misuse, loss, modification, accidental or unauthorised access or disclosure, destruction, or alteration. Security measures need to be included in any equipment used to store personal data and measures taken to ensure the integrity, reliability, and competence of personnel that has access to the personal data, with proper measures to ensure the secure transfer of personal data.

    i. The PDPA also requires that data processed for any purpose is not kept longer than necessary for the fulfilment of that purpose and it is the duty of the data user to ensure that all personal data is destroyed or permanently deleted if it is no longer required.

b) The Computer Crimes Act (1997) mentions that an individual that has unauthorised access to data held in any computer shall be liable to imprisonment for a duration of not more than five years, to a fine not more than fifty thousand ringgit, or to both.

c) The Communications and Multimedia Act 1998 (CMA), provides the following provisions when it comes to data security: -

    i. Any unauthorised access of data via network means without prior approval is subject to fine and imprisonment terms.

    ii. Any unauthorized transmission of data via network means without prior approval is subject to fine and imprisonment terms.

2.4 Data Sovereignty and Liability

a) All stakeholders that collect and utilise data from a data originator must ensure that data originators are aware of the legal jurisdiction in which their data is being stored and the legal jurisdiction in which their back-ups are being stored. As an example, if a large agriculture company decides to have all data it manages including farm data from farmers to be stored in a cloud data centre which resides in a different country, and if there are specific laws in that country that will govern the storage of this data, then this will need to be clearly communicated to the farmers.

b) In any contract that is drawn out, there is an understanding that the data originator guarantees the accuracy and completeness of the raw data to the best of their ability and knowledge. However, they are not liable for damage arising from or connected with the generation, receipt and use of this data by machines, devices, data users, and third parties.

c) However, in situations where a data originator needs to be held liable, then this must be articulated in the contract and all relevant clauses to be understood clearly and agreed upon by the data originator.

d) When determining when liability clauses should or should not be inserted into data sharing contracts, the below serves as a guideline: -

i. Data originator should not be liable when: -

- Data accuracy is not within control of data originator. For example, if weather conditions affect the accuracy of collected data, the data originator should not be held liable.
- Sharing non-regulated data as the data is being shared voluntarily for the purpose of knowledge sharing.
- Data provided by the originator is in the agreed upon format and detail level required but inaccuracies occurred due machine error such as wrongly calibrated or installed sensors.

ii. Data originator should be held liable when: -

- Data was collected in a controlled environment and data originator was in full control of accuracy levels.
- Inaccurate sharing of regulated data.
- Data provided by the data originator is not in the agreed upon format or detail level.

Relevant Existing Act Referred

a) The Personal Data Protection Act 2010 (PDPA), in covering rights for personal data, provides the following provisions when it comes to data liability: -

i. A data owner is able to formally request a data user to not begin or cease the processing of personal data if that data can cause or likely to cause damage to the data owner or another stakeholder.

ii. However, the above point will not be adhered to if the data owner had originally given consent or is required due to contractual or legal obligations.

Section 3: Case Studies

3.1 Farm X: A Smart Farm

Farm X is an AI-powered smart farm that is efficient in farm production as the smart farm is stackable, mobile, customised and utilises optimum conditions for growing crops, and can withstand external climates. Farm X is space efficient, scalable, utilises controlled lighting, uses less water, produces a stable yield unaffected by weather and has a year-round harvest. Its most relevant feature in relation to how data is being utilised is how the farm is driven by data and analytics. Farm X's live data feeds and analytics driven growing system guides crop cycles for optimal harvest. Thus, this relates to faster and more frequent crop cycles compared to traditional agriculture. The more crops Farm X grows, the more data Farm X collects. This allows Farm X to optimise and automate key parts of the system.

In this scenario, Farm X acts as a data originator by efficiently collecting and storing farm data. Utilising service providers to provide sensors as well as telecommunication services such as 5G connectivity, Farm X can also analyse its own data with the help of AI technology. Farm X should also ensure that the contracts it has with the service providers that access their data should sufficiently address how the data that they are collecting is being stored and used, along with security measures that are put in place to protect that data.

3.2 Farmer X: A Smallholder Farmer

Farmer X leases a small farm. Farmer X is the data originator for all data-related to the farm operations. Farmer X uses rented machinery for certain farming activities and manual labour for other farming activities. In this scenario, the machinery provider is the data provider. The data users would be fertiliser manufacturers that receive information about the types of fertiliser needed and composition of the fertiliser, and the government for production data. Another data user would be the retail value chain, such as the packaging and sales team, as well as resellers of the crops whereby they would have production data based on the crop yields.

There may be instances where smallholder farmers may not have any concerns or interest in how their farm data is used and stored. At the minimum, the farmer should be notified that their data is being processed and shared, including the disclosure of its purpose. Data providers and data users should also practice proper storage and secure data processing of farm data. In addition, data providers and data users should disclose the rights of farmers (who are the data originators) regarding their rights to deletion of data and rights to control of how their data is being used.

3.3 Research Centre X: A Smart Farming Technology Research Centre

A smart farming technology research centre conducts research on farming methods utilising modern farming technology that can help contribute towards an increase in quantity and quality of agriculture products. The various areas of research investigated by the centre includes agriculture automation, smart cultivation practices, green and zero waste technology, remote sensing, soil scanning, and IoT. With this information, a smart farming community centre is set up to upskill farmers on how to use technology to manage their farms better and to increase yield per hectare.

Here, the farmer plays the role of data originator, while the research centre plays the role of third-party professional advisors. The research centre also plays the role of data user as farm data collected has also been utilised for research papers that have been published by the centre. In this scenario, it would be good for any data sharing contract in place to include liability clauses as the farm data has been utilised to produce research papers. To continuously motivate farmers to continue to share data, farmers should be assured that any inaccuracy arising from their data is not bound to any damages or penalty clauses.

3.4 Tool X: A Palm Oil Traceability Tool

Tool X is an online open access tool that allows anyone to trace Company X's palm oil supply chain down to the plantation and mill level. It is a traceability tool that provides a clear and transparent view on Company X's supply chain origins and processes. Specifically, the tool provides information on ownership of each mill and allows users to view a satellite imagery that tracks changes in the forest. This addresses concerns about deforestation and increases accountability.

In this scenario, the plantations and mills that serve Company X act as the data originators feeding the required information into the tool. Company X is the data provider as it provides traceable data to anyone who accesses the tool. Investors, the government, and customers are the data users as they process and analyse the data obtained from plantations and mills. As the data becomes available to anyone who accesses the tool, it therefore becomes important that key elements of the data sharing code of practice around data ownership, data sharing, data trust and data liability are incorporated in the data sharing contract between Company X and the plantations and mills under its purview.

3.5 Platform X: An Agriculture Platform

Platform X is a platform that connects agriculture stakeholders in the agriculture value chain. Farmers, agricultural suppliers, wholesalers, retailers, and agricultural consumers can obtain information on local weather conditions, farming practices, location of raw materials and location of product supplies. Farmers can retrieve information through this agricultural mobile application platform that acts as a knowledge base.

In this scenario, the platform service provider should clearly define parameters to explain to data originators on which information they can share publicly, which information is for their personal view, and which information is shared with several named stakeholders. This is to avoid oversharing of data. With this, the platform service provider needs to have proper access control management to avoid data leaks and should also ensure secure data storage with the intention of avoiding unwanted data breaches.