Designing an effective data-sharing framework for AgriStack

Anita Gurumurthy, Nandini Chami, Rudraksh Lakra

Policy Brief

May 2025

The research for this publication was carried out by **IT for Change** with support from the European Commission, Friedrich Ebert Stiftung, and the Australian Government, Department of Foreign Affairs.

About IT for Change

Founded in 2000, IT for Change is a Southern, women-led NGO rooted in feminist principles and driven by a commitment to social justice. Recognized with Special Consultative Status by the Economic and Social Council of the United Nations. IT for Change is dedicated to democratizing digital technologies, enabling individuals and communities to harness their power for empowerment.

Credits

Research and writing: Anita Gurumurthy, Nandini Chami, Rudraksh Lakra
Editorial review: Sadhana Sanjay
Proofreading: Susan Sreemala
Design and layout: Susan Sreemala
Cover design: Harikrishnan B.

393, 17th Main Road,
35th Cross Rd, 4th Block,
Jayanagar, Bengaluru,
Karnataka, India-560041
www.itforchange.net

For publications enquiries, please contact comms@itforchange.net

Supported by

Co-funded by the European Union

Friedrich Ebert Stiftung

Australian Government
Department of Foreign Affairs an

Table of Contents

1. Overview: Dimensions of an effective data sharing framework for an agricultural data exchange

Trusted and standardized data sharing can transform the agriculture sector by enabling effective and efficient data-based decision-making that enhances agricultural productivity, boosts farmers' incomes, and strengthens policy preparedness towards shaping climate-resilient food systems.[1] This is the promise that the government of India's AgriStack initiative seeks to fulfil by creating a national-level data space in the agriculture sector that facilitates secure, trusted, transparent, and responsible data sharing for public and private sector-led data-driven innovation. AgriStack is envisioned as an aggregate architecture of various databases, registries, data standards, APIs, and policies with appropriate regulatory frameworks governing data sharing.

Lessons from the experience of the Common European Agricultural Data Space (CEADS) demonstrate that the design and implementation of the data-sharing framework is vital. This will enable the elimination/minimization of data harms and maximization of benefit-sharing from data innovation dividends for all participants in the agriculture data exchange.[2] A binding, sector-specific data sharing framework that straddles both personal and non-personal data governance considerations is critical for a comprehensive approach. The following considerations[3] need to be taken on board, in an integrated manner:

- Privacy and security: Guardrails for privacy violations stemming from the re-identification of individuals in data processing and protection against breaches of sensitive data
- Data rights of farmers as data originators: Rights to access data, control the sharing of data, and the right to benefit from third-party use of data for innovation.
- Transparency and accountability in data sharing: Clear contractual agreements and licensing conditionalities that specify obligations and liabilities of all parties accessing datasets from the agricultural data exchange.

[1] iSHARE EU (2025). Boost Agriculture with secure data sharing. https://ishare.eu/news/2025/04/02/cultivating-growth-how-trusted-data-sharing-transforms-agriculture/

[2] Farmers/ producers, data intermediaries, technology services providers, and public sector agencies

[3] Ryan et. al (2024). The future of agricultural data-sharing policy in Europe: stakeholder insights on the EU Code of Conduct. https://www.nature.com/articles/s41599-024-03710-1

2. Key issues/concerns about evolving an effective data sharing framework for AgriStack

2.1. The imperative to recognise the rights and claims of farmers as data originators

Data originators refer to the individuals and entities whose actions result in the collection and creation of data. In the collection of agricultural data, there are quite a lot of challenges in determining who the data originators are, as often, there are multiple parties involved. For example, in the EU, as the Data Act is moving into the implementation phase, concerns about how to apportion rights in farm-related non-personal data (soil health, moisture, fertility, and so on) between individual farm owners and owners of farm machinery/ IoT on the lands of these farmers have emerged. Currently, the Data Act recognizes data claims of farmers only in instances where farmers own/have a lease on the farm equipment from which data is being collected. This results in a legal vacuum for the data claims of those farmers who have entered into agreements with agricultural technology providers (ATPs) for a data-related service from a machine operator (for instance, for harvesting operation) even when there is no sale or lease contract for IoT devices.[4] The asymmetries of power between farm owners and powerful ATPs in this context lead to dependencies for the farmer, with vendor lock-ins making opt-out difficult, if not nearly impossible. It is important for AgriStack, given the context of India's agriculture sector where the bulk of landholdings are of small and marginal acreage, to program for the recognition of farmers as data originators from the get-go–particularly in relation to the non-personal data footprints collected from their land parcels–to enable them to assert autonomy and control over sharing and re-use.

Such a legal framing of 'data originator' rights will also provide a robust scaffolding/ necessary complementarity to existing personal data protection legislation, particularly in the context of protections against individual and group profiling in the processing of publicly available agricultural datasets, which are mixed data sets. For example, many mixed datasets in the farm sector containing farmer personal data, such as the Record of Rights, Tenancy, and Crops (RTC), are already in the public domain. These publicly available datasets are exempt from the scope of the Digital Personal Data Protection Act, 2023 ("DPDPA").[5] In the absence of safeguards, agricultural technological providers–such as a micro-crop insurance or micro-credit service provider–could utilize these datasets to build solutions that result in rights-violating farmer profiling. Mixed data sets, even when the personal data they include are anonymized, could enable discriminatory individual and group profiling, influencing credit, insurance, or subsidy

[4] Ryan, M., Atik, C., Rijswijk, K. *et al.* (2024). The future of agricultural data-sharing policy in Europe: stakeholder insights on the EU Code of Conduct. *Humanit Soc Sci Commun* **11**, 1197. https://doi.org/10.1057/s41599-024-03710-1

[5] Government of India. (2023). Digital Personal Data Protection Act, 2023, Section 3(c)(ii). Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

access adversely for vulnerable groups.[6] A data originator's right can be a useful claim to fix this problem, as it would mean that prior to the re-use of publicly available mixed data sets about farmers and their land parcels, a consultation process for informed and free consent would become mandatory.

2.2. The need to build an enabling environment that incentivizes data sharing, particularly from the private sector

In India's AgriStack, it is imperative to ensure that the data sharing environment does not end up as a one-way street where Open Government Data in the domain ends up subsidising business models, with little or no utility to farmers who consume these services.

The emerging regulatory framework in the EU for its common health data space is notable for the following features:

- A system of 'data permits'. This system ensures that requests for data access from the exchange meet a particular threshold of public value generation, and only those requests that pass the test for socially beneficial innovation are permitted.
- Recognition of the distinctions in data processing between primary and secondary uses, when deciding permissibility thresholds. Primary use refers to data processing for the provision of a personalized service to the data originator, while secondary use refers to data processing of aggregated datasets for research, future innovation, and public decision-making (uses where the data processing may not directly lead to benefits for the data originator). Fairness of consent procedures and safeguards may be a sufficient threshold in processing data for primary uses, but this cannot be the case for secondary uses (where data subject X may also be affected by downstream profiling even if the said service or innovation is not built on datasets that include X's data).
- The baseline of a reciprocity principle to ensure that those who take data also give back to the pool. The proposed regulatory frame for the EU's common data space in health specifies that "Where a data holder has received enriched datasets following a processing based on a data permit, it shall make available the new dataset back into the data pool" to enable a multiplier effect. Such mandatory data sharing obligations–particularly of NPD–have been found valuable for public decision-making in different sectors, including health and transportation. And in the case of AgriStack, where OGD is likely to be the bulk of initially available datasets, a reciprocity obligation on the private sector to contribute enriched datasets back to the pool is critical to build both data volume and veracity and ensure innovation multiplier effects.

[6] Dasari, Prasanna. (2025). Digital Lending in India: Harassment, Settlements, and the Rise of Financial Exploitation (January 01, 2025). Available at SSRN: https://ssrn.com/abstract=5092390 or http://dx.doi.org/10.2139/ssrn.5092390

3. Key recommendations for AgriStack's data sharing framework

Based on the two insights above–that data rights of farmers as data originators and the social good/public value proposition of data innovation, both need to be preserved in AgriStack–we recommend the below:

3.1. Guardrails for privacy and safeguards against automated profiling

The data sharing framework must institute clear accountability obligations on the entities accessing datasets from AgriStack to address the risks of privacy violations in data processing (e.g., data breaches that result in re-identification). All forms of data processing must comply with the Supreme Court's judgment in Justice K. S. Puttaswamy (Retd.) v Union of India (2017), which underscores that any interference with the right to privacy should comply with the principle of proportionality, which entails legality (statutory authorization), suitability and narrowly tailored use, and balancing.[7] Justice Chandrachud's opinion in the case underscored the need for the conduct of both private and public entities to be grounded in the principle of proportionality.[8] Safeguards for aggregate data processing should use the DPDPA as a baseline and build upon it to address its limitations and adapt data protection to the specific context of agriculture.

Given that predictive behavioural modelling in AI – involving mixed data sets – can introduce data fields that render individuals from certain social groups highly vulnerable to exclusion and social control, protections against automated profiling become essential.[9] In every instance of data access from the AgriStack, it is important to ensure:

- Ex-ante screening of proposed use cases of data to identify risks of discriminatory profiling. This is particularly important in cases where the data being processed falls within the categories of publicly available data under DPDPA Section 3(c)(ii), such as RTC datasets, that often include vast amounts of personal data.

- Guidelines for Agri-Tech Service Providers (ATSPs) on the algorithmic design of predictive AI models. The consent manager is not a sufficient solution to protect data originators and others affected by AI-based decision-making against discriminatory outcomes. Additional guidelines, therefore, become essential.

[7] Supreme Court of India. (2017). Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. https://indiankanoon.org/doc/127517806/

[8] Ibid. per Chandrachud, J., at [180]. https://indiankanoon.org/doc/127517806/

[9] Ploug, T. (2023). The right not to be subjected to AI profiling based on publicly available data—privacy and the exceptionalism of AI profiling. Philosophy & Technology, 36(1), 14. https://link.springer.com/article/10.1007/s13347-023-00616-9

- Transparency and accountability benchmarks. It would be important to place an obligation on agricultural technology providers to design their systems in a way that the outcomes of algorithms are explainable. In their data agreements, ATSPs should be obligated to clearly specify the data collection process, list of personal and farm data that are collected at the farms, and inform farmers of how their data is used.[10]

3.2. Rights of farmers as data originators

In the primary uses of data, where farmers share their datasets in return for specific data-based services from technology providers, there must be a clear bottom line that the rights of farmers as data originators cannot be waived away in the contractual agreements/terms of service that they sign.[11] We are recommending the framing of "data originators" rather than using the formulation of "data principals/data subjects" as this will address the question of the rights of farmers to the non-personal datasets generated in their environment.

As data originators, farmers should be guaranteed the following rights:

3.2.1. Right to Data Access: As data originators, farmers must have a right to access all data generated by them from their socio-behavioural and socio-environmental interactions, as well as the relevant metadata necessary to interpret and use that data, in all instances of primary use of their data. Correspondingly, the relevant data holder (public/private entity) with whom they are in a data sharing agreement/contract for receipt of services must bear a duty to provide such access.[12] It would be desirable to link data rights in personal data to the concerned individual, and rights in non-personal data to specific "farm units"[13] in order to ensure continuity in NPD rights.

3.2.2. Right to be consulted and determine the extent of data sharing in both primary and secondary use cases: As data originators, farmers must be consulted in every instance of primary use of their data. Consent management modalities cannot operate under a blanket consent fashion, whereby consent given once, or for a certain purpose/dataset/entities, is deemed sufficient across purposes/datasets/entities. Such blanket consent infringes upon informational self-determination – a key aspect of the right to privacy recognized in Supreme Court jurisprudence – as it dilutes the ability of the data originator to control how and by whom

[10] Kaur, J., Hazrati Fard, S. M., Amiri-Zarandi, M., & Dara, R. (2022). Protecting farmers' data privacy and confidentiality: Recommendations and considerations. Frontiers in Sustainable Food Systems, 6. https://doi.org/10.3389/fsufs.2022.903230

[11] ibid.

[12] EU Data Act (2024), Article 3(1) and 4(1); Atik, C. (2022). Towards Comprehensive European Agricultural Data Governance: Moving beyond the "data ownership" debate. International Review of Intellectual Property and Competition Law (IIC), 53, 701–742. https://doi.org/10.1007/s40319-022-01191-w; EU Code of conduct on agricultural data sharing by contractual agreement (2020) Page 9-10.

[13] ibid.

their data is processed.[14] Thus, it is essential to add friction to downstream data flow, such as purpose limitation and data minimization, which are principles recognized as essential for data processing by the Supreme Court in Justice K. S. Puttaswamy (Retd.) v. Union of India (2019).[15]

Further, certain explicit restrictions may be necessary, such as limiting the processing of personal data or NPD in ways that could have adverse economic, social, civil, or political impacts on data users — here, specifically farmers and communities (eg. 'reverse redlining'[16] in micro-credit or micro-insurance services where marginal and small farmers risk facing extremely adverse terms such as high interest rate/premium). Another key aspect is ensuring that ATDPs providers do not subvert or impair farmers' autonomy, decision-making, or choices when exercising their rights through manipulative design features (dark patterns) in digital interfaces.[17] It may, in fact, be necessary to augment technical consent management applications with human-in-the-loop mechanisms such as data intermediaries or trusted third parties to manage access requests transparently and fairly. This will go a long way in fostering trust among stakeholders.[18] Farmer Producer Organizations (FPOs) are well-placed to carry out this function, as they hold the trust of the community and represent their collective interests.[19] This can promote fair and accountable processing of farmer data while curbing unilateral exploitation and collective profiling.

In instances of secondary use, a consent management modality may be difficult to implement. Therefore, in these instances, for example, when aggregate agricultural domain datasets are being processed for research and innovation, the AgriStack data sharing framework must recognize the right of the public (a societal right) to be informed about the uses of such datasets. This will include the right to public consultation and other rights for ongoing scrutiny and audit. This is similar to the societal rights to participate in environmental decision-making matters as guaranteed under the Aarhus Convention, so that unanticipated harms can be examined and publicly deliberated. In a context such as India, where the majority of farmers are small and

[14] *Justice K.S. Puttaswamy v. Union of India* (UOI) MANU/SC/1054/2018 ("Puttaswamy II") (A.K. Sikri, J. Majority Opinion) [232](v) and [446](m)-(n); Puttaswamy I (D.Y. Chandrachud, J opinion) [180], [190]; Puttaswamy I (Rohinton Fali Nariman, J. Opinion) [364]; *Puttaswamy I* (Sanjay Kishan Kaul, J. Opinion) [473]; [481].

[15] Supreme Court of India. (2018). *Justice K. S. Puttaswamy v. Union of India (UOI)*, MANU/SC/1054/2018, per Sikri, J., at (d). https://indiankanoon.org/doc/127517806/

[16] Wikipedia contributors. (2025, August 9). *Redlining*. In *Wikipedia*. https://en.wikipedia.org/wiki/Redlining

[17] European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act), arts. 4(4), 5(4). Official Journal of the European Union, L (2023/2854). Entered into force January 11, 2024; Central Consumer Protection Authority (India). (2023, December 4). Guidelines for Prevention and Regulation of Dark Patterns, 2023. Ministry of Consumer Affairs, Food and Public Distribution.

[18] European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), arts. 10–12. Official Journal of the European Union, L 152, 1–44. https://data.europa.eu/eli/reg/2022/868/oj

[19] Kumar, R., Desai, V. S., & Koshy, N. S. (2023, December). *Creating sustainable data cooperatives in the Global South: Frameworks for institutional support*. IT for Change. Retrieved from https://itforchange.net/index.php/creating-sustainable-data-cooperatives-global-south-frameworks-for-institutional-support

marginal land owners and socio-economically vulnerable, the AgriStack must introduce clear guidance on how public consultations with affected communities must be carried out.

3.2.3 Right to data portability: As data originators, in all instances of primary use, farmers should be guaranteed a right to portability[20] in both historical and real-time datasets, as well as essential inferences in the form of processed data in order to ensure that farmers are able to switch ATPS or platforms with seamless functionality and without loss of service quality or switching-costs.

3.3. Obligations for mandatory data sharing

Private entities may hold valuable datasets in the domain, including inferential data that are critical to determine state policy decisions in areas such as addressing climate resilient food systems, emergency measures to safeguard farmer interests in crop failures, and other public interest imperatives. Under the EU Data Act (2024), such mandatory public access is limited to emergency situations or narrowly defined grounds where specific data is identified, less restrictive measures to achieve the intended goals have been exhausted, and the data is absolutely necessary to fulfil a specific task carried out in the public interest.[21] Notably, the obligation to comply with such public access requests is placed on dominant market players and does not extend to microenterprises and small enterprises. The AgriStack data sharing framework must deliberate upon the introduction of a mandatory data sharing obligation on private players in such cases, which extends to accessing inferential data that may otherwise be inaccessible owing to IP barriers.

3.4. Regulatory Body for AgriStack

Similar to the proposal in the EU for the governance of the Common Health Data Space, it is important for the AgriStack Data Sharing Framework to set up an AgriStack regulator – an Agriculture Data Access Board, through the introduction of a sector-specific regulation. This will ensure that the data sharing space has appropriate statutory backing to ensure compliance with the constitutional principle of legality[22] along with clear delineation of the regulator's mandates and functions. The Agriculture Data Access Board must be tasked with the following responsibilities:

- Creation of a metadata registry of all participants in the AgriStack, which will ensure visibility for all participants on which types of data reside with which actors and enable the placement of data access requests to the Board

[20] Atik, C. (2022). Towards Comprehensive European Agricultural Data Governance: Moving beyond the "data ownership" debate. International Review of Intellectual Property and Competition Law (IIC), 53, 701–742. https://doi.org/10.1007/s40319-022-01191-w

[21] EU Data Act (2024), Article 15.

[22] Supreme Court of India. (2017). Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

- Data access requests that are submitted must go through an evaluation process, where risks to fundamental rights and public interest are evaluated, with separate guidelines for applications for primary use (data collected to provide services to farmers) and secondary use (aggregate data processing for future research and innovation). FPOs and farmer organizations may be empanelled in the assessment of data access requests.
- Where data access requests are approved, data permits may be issued by the Board. A data permit confers the right to access and process data to the data requester and cannot exceed more than 5 years. A data permit must carry details of the general conditions applicable to the data requester on the data made available under the permit, including types and format of data accessed and their sources, purpose, duration, technical characteristics and tools, fees to be paid, and transparency and accountability obligations.
- Data permits must include an obligation on the data requester to clearly specify how their model is addressing the risk of discriminatory profiling.
- Grievance and redress mechanisms for aggrieved parties must be constituted.
- A Data Literacy and Help Desk public service should be set up for guidance to protect farmers' interests and educate farmers about their data rights.

A fair, future-ready data-sharing framework for AgriStack must underwrite the data rights of farmers as data originators, ensure equitable benefit-sharing in data-based innovation trajectories, and establish robust safeguards against privacy harms and discriminatory profiling. Embedding principles of transparency, accountability, and mandatory reciprocity obligations in data sharing will be crucial to fostering trust and enabling inclusive, public-interest-driven innovation in agriculture. The establishment of a dedicated regulatory body is equally essential to enforce compliance and safeguard the public interest. By adopting these measures, AgriStack can evolve into a genuinely transformative platform — one that enhances agricultural productivity while upholding farmer autonomy and advancing equitable, just data governance in India's agricultural sector.