Agriculture & AgriTech

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For AgriTech platforms, agricultural financial services, farming input companies, and drone/satellite services.

1. Overview & Applicability

The agriculture sector is undergoing rapid digitisation — from e-NAM marketplaces to precision farming apps and agri-credit platforms. Farmers are now Data Principals whose land records, crop data, income details, and location data are being collected at scale. AgriTech companies must implement DPDPA compliance thoughtfully, recognising that many farmers have limited digital literacy. Privacy notices and consent must be in the farmer's regional language.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Farmer Data	Name, village, land survey number, crop type, income, bank account for DBT — personal data.
Land Records	Survey numbers, ownership documents, encumbrances — sensitive land and identity data.
Crop & Yield Data	Satellite or drone-derived crop monitoring data linked to a specific farmer — personal data.
Agri-Financial Data	KCC loan records, crop insurance claims, PM-KISAN beneficiary data — financial personal data.
Digital Literacy Consideration	Consent obtained from farmers must be genuinely informed — use regional language, voice-based consent where appropriate.
Data Processor	Input companies, FPO aggregators, crop insurance companies receiving farmer data — require DPAs.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Language-Appropriate Consent**
   Consent forms must be available in the farmer's regional language. For low-literacy contexts, use voice-based or assisted consent mechanisms. Document carefully.
2. **Land & Crop Data Governance**
   Land survey data and crop information linked to a farmer is personal data. Collect only what is needed. Do not share with private parties (input companies, lenders) without explicit consent.
3. **Agri-Finance Data**
   Loan application data, KCC records, and crop insurance claims must be kept secure, accessed only by authorised personnel, and not shared with marketing teams.
4. **Drone & Satellite Data**
   Remote sensing data identifying specific farm parcels linked to named farmers is personal data. Disclose collection method and obtain consent where individual farmers are identifiable.
5. **PM-KISAN & DBT Data**
   Government welfare data (Aadhaar-linked DBT, PM-KISAN beneficiary data) is sensitive. AgriTech platforms acting as intermediaries must execute DPAs with the government body.

6	**FPO & Aggregator Data** Farmer Produce Organisations collect members' personal and financial data. Implement governance structures and obtain member consent.
7	**Market Price & Trading Data** Data on individual farmers' transactions on e-NAM or commodity exchanges requires consent before sharing with analytics or financial service providers.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Translate privacy notices and consent forms into all regional languages relevant to your farmer base.
- ☐ Implement voice-based or assisted consent for low-literacy farmer contexts.
- ☐ Audit all farmer data collected — land records, crop data, financial data, location data.
- ☐ Execute DPAs with input companies, insurance providers, banks, and FPO aggregators receiving farmer data.
- ☐ Restrict access to farmer Aadhaar, PAN, and bank data — only authorised DBT/credit personnel.
- ☐ Build a farmer rights mechanism — allow access to their profile, loan records, and request corrections.
- ☐ Appoint a Grievance Officer accessible via toll-free number and local language support.
- ☐ Review drone and satellite data programmes — ensure individual farmers are notified of data collection.
- ☐ Train field agents and agri-loan officers on farmer data rights and DPDPA obligations.
- ☐ Implement data security for all farmer data stores — encryption and access controls.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Farmer Data Inventory** Catalogue all farmer data collected across your platform — registration, crop, financial, and location data.
2	**Month 2: Language Adaptation** Translate all consent and notice materials into relevant regional languages.
3	**Month 3: Vendor DPAs** Execute DPAs with all input companies, banks, insurance partners, and government bodies.
4	**Month 4: Rights Mechanism** Build farmer rights request channel — accessible by phone, IVR, or field agent assistance.
5	**Month 5: Security** Implement encryption for all farmer financial and identity data stores.
6	**Month 6+: Field Training** Train agri-loan officers, field agents, and FPO staff on DPDPA obligations.

🌾 Farmers are often unaware of their digital rights. Your DPDPA compliance must go beyond legal boxes — make privacy notices genuinely understandable in local languages and use assisted consent where needed.