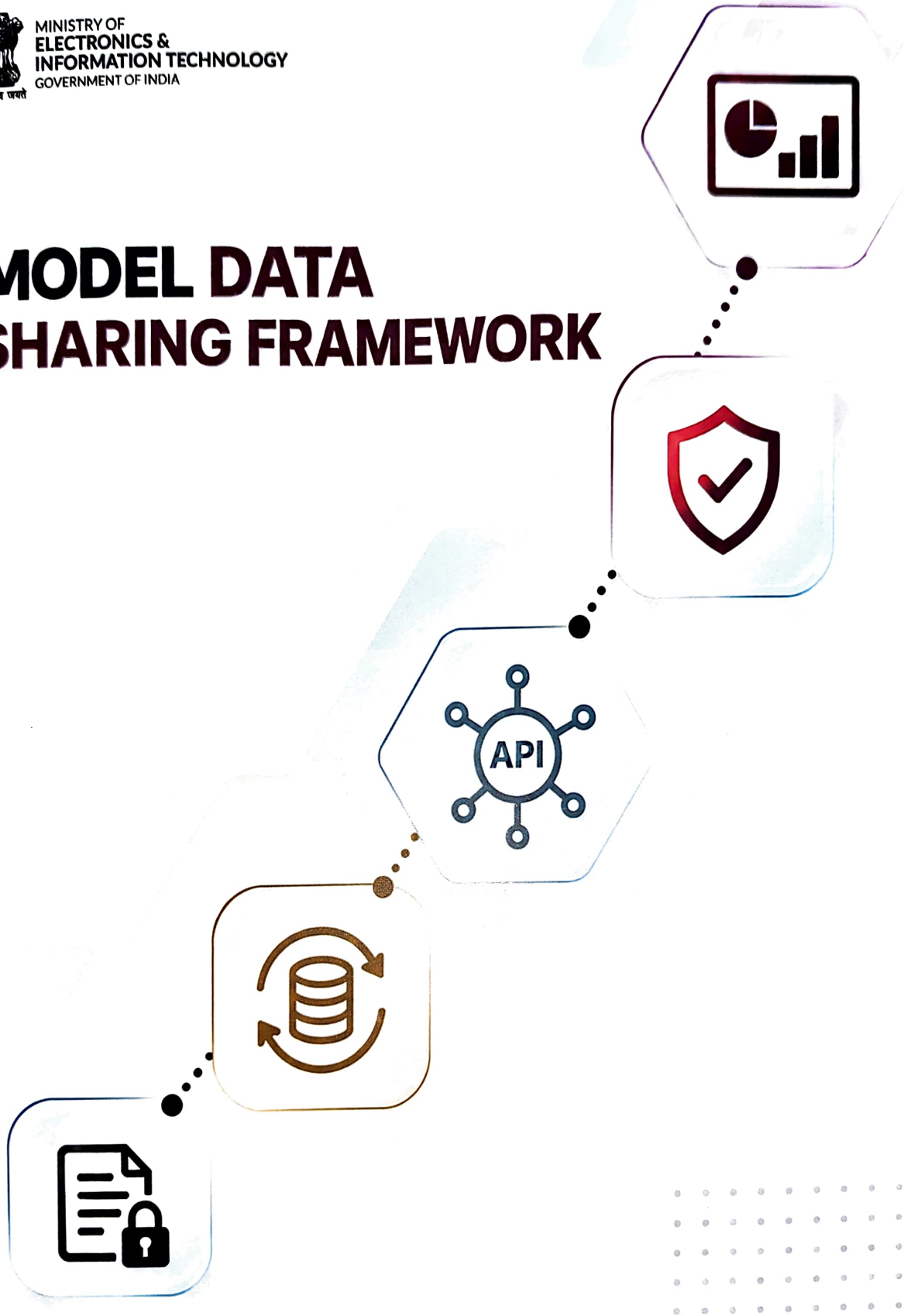
MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

MODEL DATA SHARING FRAMEWORK



September, 2026

Table of Contents

1. Introduction 2
1.1. Purpose 2
1.2. Applicability 2
1.3. Objectives 2
1.4. Main Stakeholders 3
2. Data Sharing Principles and Best Practices 3
2.1 Part A - Data Sharing Principles 3
2.2 Part B - Data Sharing Safeguards 4
2.3 Part C - Best Practices 4
3. Different Types of Shareable Datasets of the MDO 6
4. Different Modes of the Data Sharing 7
5. Data Sharing Requisite 8
5.1. Data Classification Framework 8
5.1.1 Classification Register 8
5.1.2 Example - Dataset having Personal Information (Indicative) 8
5.2. Dataset Inventory Register 9
5.3. Data Sharing Platforms 10
5.4. Data Sharing Governance and Approval Process 11
5.4.1 Data Governance Committee 11
5.4.2 Approval Process for Access to Datasets 11
5.4.3 Pre-requisite for sharing data with Data Requestor / Data Recipient 12
5.4.4 Application form for Data Requestor / Data Recipient 13
5.4.5 Terms of data usage and data sharing agreement 13
5.4.6 Purpose Code Framework 14
5.5. Data Access Charges (Indicative) 15
5.6. Grievance and Complaint Redressal 15
6. Review 16
Annexure I: Log Record Format 17
Annexure II: Techniques for Data Anonymisation 18
Annexure III: Sample Application Form by Data Requestor 19
(1) Application Form for Central MDO, State and UT As Data Requestor 19
(2) Application Form for Private Sector, Start-ups, Academia, Research Organisation 20
(3) Purpose Code (Indicative) 21
Annexure IV: Sample Memorandum of Data Compliances 22
(1) Memorandum of Data Compliances (For API data sharing) 22
(2) Memorandum of Data Compliances (For Portal-based data sharing) 24
(3) Memorandum of Data Compliances (For Bulk data sharing) 25
(4) Memorandum of Data Compliances (For Citizen sharing) 26
Annexure V: Sample Data Sharing Agreement 27
List of Abbreviations 35

1. Introduction

The Model Data Sharing Framework is prepared in pursuance of the decisions made by the Committee of Secretaries (CoS) in its meeting held on 15 May 2026 on Interoperable and Integrated Government Databases. This framework gives effect to the decision, which directs every Central Ministry, Department, and attached office to consider publishing a Data Sharing Procedure within 12 months.

While preparing the Model Data Sharing Framework, the reference has been drawn from existing data sharing policies, open API policy, the data sharing guidelines published by the Government (DST, Meity, MoRTH, NHA and States). The idea is to assist the Ministry / Department / Government Organisation [MDO], who can customize this model framework appropriately while preparing specific MDO-wise Data Sharing Framework / Procedure.

1.1. Purpose

The Data Sharing Framework is to facilitate data sharing by [MDO] within and outside the government. It outlines how MDO and its ecosystem partners process and use digital data and complies with the Information Technology Act, 2000 (IT Act), Aadhaar Act, 2016 and the Right to Information Act, 2005 (RTI Act), Digital Personal Data Protection Act, 2023 (DPDP Act), other applicable laws and rules and regulations thereunder.

These guidelines are to be read with, and not in contradiction to any applicable law, or any instrument having the force of law, and shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable laws (mentioned above), sectoral rules, regulations and other binding agreements having the force of law.

1.2. Applicability

This framework applies to datasets produced, collected, or held by [MDO] and its attached offices and subordinate organisations. Datasets classified as national-security-sensitive, Cabinet-restricted, or otherwise non-shareable under statute are governed by Category 4 (Non-Shareable) and fall outside the sharing framework set out here.

The Ministry / Department / Government Organisation [MDO] should adopt this model framework and customise it appropriately to prepare their data sharing procedure.

1.3. Objectives

The key objectives of the framework is to:

1. Enable evidence based and data driven decision making at whole-of-the-government level by sharing data within the government
2. Improving ease of living and ease of doing business such that individuals and entities are not asked to share physical paper but share digital data
3. Provide an adequate guidance framework for the secure handling of the digital data (personal and non-personal data of the beneficiaries, entities and others) in compliance with laws and applicable consent.
4. Establish an institutional mechanism for sharing data with any entity requesting data for specific purposes as defined under these guidelines.
5. Support data sharing through digital means (data exchange platforms and/or data sharing portals)
6. Enhance API economy in the country and strengthen innovation and startup ecosystem
7. Support research and development by making available bulk non-personal data to institutions
8. Enhance awareness regarding the importance of data sharing along with data privacy and data protection to instill a privacy-oriented mind-set

1.4. Main Stakeholders

The main stakeholders are as follows:

1. Ministry / Department / Government Organisations
2. Citizens
3. Private Organisations - Companies, MSMEs, Start-ups, etc
4. Research and Academic Organisations

2. Data Sharing Principles and Best Practices

All sharing, access, disclosure, publication, transmission, use or other processing of data under this Framework shall be governed by the following principles and shall apply to Central Government Ministries, Departments, statutory authorities, autonomous bodies, public sector entities, implementation agencies, service providers, processors and authorised recipients. This may also be adopted by State's / UT's Data Governance Committee for State Governments and Union Territory Administrations and its organisations.

2.1 Part A - Data Sharing Principles

Principle 1: Data Sharing by Design. MDO (Ministry / Department / Government Organizations) to use this framework to share dataset by design. Non-sharing should be treated as the exception.

Principle 2: Sharing for Data and Evidence-Based Governance. The first purpose of sharing is better governance: sharper targeting of schemes, minimisation of inclusion and exclusion errors, real-time monitoring, impact evaluation and timely course correction. MDO should share not only statistical abstracts but the administrative datasets, beneficiary counts, facility-level service metrics, expenditure data, on which evaluation actually depends.

Principle 3: Granular and Machine-Readable Data. Aggregate, anonymised data shall be published at the most disaggregated administrative unit feasible, preferably the village or ward, preferably coded under the Local Government Directory (LGD), for decentralised planning is impossible without it. Data shall be published in open, machine-readable formats.

Principle 4: Interoperability and Discoverability. MDOs shall adopt metadata & data standards, standard code directories, unique identifiers and data dictionaries so that datasets can be joined, compared and reused, collected once, used many times. MDO should have inventory of datasets and directory of dataset qualifying for sharing should be available in public domain, at portal as well as data exchange platforms.

Principle 5: Frictionless Sharing Within Government. Sharing between Government entities should be treated as internal transfer and internal use, not disclosure. MDO shall access one another's data through secure APIs and standing data-sharing protocols for defined official purposes, without case-by-case objections, file references or discretionary gatekeeping. Purpose logging and audit trails shall replace prior permission as the mechanism of control.

Principle 6: Tiered Sharing Outside Government. People outside government - citizens, researchers, civil society and industry can get access in three tiers:

1. Open: anonymised, aggregate data anyone can download under an open licence
2. Registered: available after signing in and stating why you need it
3. Restricted: available only on approval and after signing a data-sharing agreement

Inside the government, sharing helps citizens through better administration. Outside government, it helps through transparency, research and innovation. Both are valid reasons to share.

Principle 7: Data Monetisation. The charge shall be nominal so as to ensure cost recovery, maintenance and avoid frivolous repeated data ask. The charge for data sharing and commercial usage shall be decided by MDO appropriately taking into consideration existing statutory rules and equivalents.

2.2 Part B - Data Sharing Safeguards

Principle 8: Compliance to law. Personal identifiable information (PII) can be shared only with the informed consent of the data principal, or under explicit legal authorisation, in conformity with the Digital Personal Data Protection Act, 2023 and data sharing should be in accordance with sectoral regulations. Definitions on data, PII data and data stakeholders should be referred to as per Act and regulations.

Principle 9: Security with Two-Way Accountability. Datasets shall be protected by encryption, role-based access control, audit trails and breach-notification protocols, and maintained to published standards of accuracy, completeness and timeliness with declared update calendars. Every dataset shall have a named Data Owner accountable both for disclosure and, equally, for justified refusal or delay in sharing.

2.3 Part C - Best Practices

1. Audit Trail

Each Ministry / Department / Government Organisation and Data Exchange Platform will maintain a secure, tamper-evident and time-stamped audit trail for all data sharing activities undertaken under this Framework. The audit trail shall record, at a minimum, the identity of the requesting entity, approving authority, purpose of sharing, dataset accessed, category of data, date and time of access, mode of sharing, data fields shared, volume of records accessed, API calls / downloads / exports, user credentials or system identity, and any modification, deletion or onward transmission of data.

Audit logs shall be protected against unauthorised access, alteration or deletion and shall be retained for a minimum period of <x> years, or for such longer period as may be required under applicable law, audit requirement, investigation, litigation hold or contractual obligation. **(Annexure I)**

2. Anonymisation and De-Identification for Bulk Data

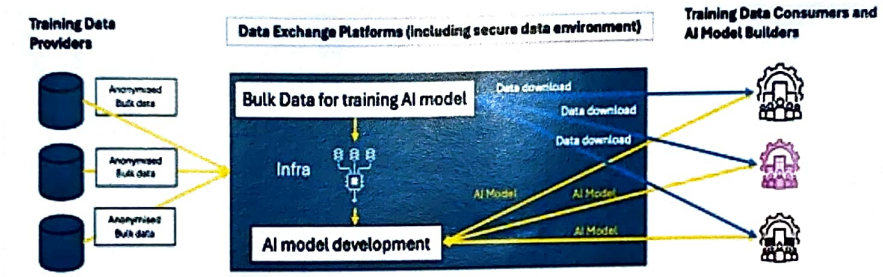
There can be two options.

In the first option, the anonymisation is the responsibility of training data providers, while, data consumers / data requestors get the data to download as well as the option to make use of a secure data environment (of data exchange platform) for AI model training and testing.

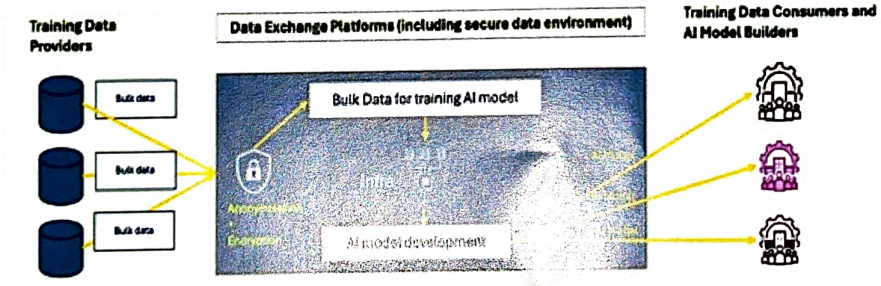
In the second option, the anonymisation and encryption of raw data (as provided by data providers) is handled by Data Exchange Platform, wherein, data consumers / data requestors get the access to data in a secure data exchange environment for AI model training and testing.

The anonymisation techniques can be seen at **Annexure II**.

Option 1: Data Exchange Platform getting anonymized data from data providers



Option 2: Data Exchange Platform handling anonymisation of raw data as received from data providers



Personal Identifiable Information (PII) Removal Checklist (Indicative)

Before any bulk release, the following steps must be completed and documented:

A. Remove direct identifiers - name, Aadhaar, PAN, mobile, email, passport number, voter ID, driving licence number, vehicle registration, and account number.
B. Generalise quasi-identifiers - convert date of birth to age band; replace full address with district/state; generalise income to range; suppress employer name.
C. Suppress or aggregate sensitive attributes - caste, religion, health condition, disability, criminal record, financial distress, migration status.

3. Sharing of anonymised and de-identified data

Anonymised, aggregated or de-identified datasets may be shared for approved public interest, research, innovation, policy analysis, service delivery improvement or AI / ML use cases, subject to the classification, approval and safeguard requirements prescribed under this Framework. Prior to sharing, the concerned CDO / nodal officer shall ensure that direct identifiers have been removed, quasi-identifiers have been generalised or masked, and the risk of re-identification has been assessed and minimised.

4. Data breach and incident management

Each Ministry / Department / Government Organisation shall establish a documented data breach and incident management procedure for identifying, reporting, containing, investigating and remediating any unauthorised access, disclosure, alteration, loss, misuse, re-identification, onward sharing or security compromise involving data shared under this Framework. Action may be taken under provisions of DPDP Act, IT act and applicable sectoral regulations.

5. Capacity Building and Awareness & Communication

Each Ministry / Department / Government Organisation shall undertake periodic capacity building and awareness activities for officials, system owners, CDOs, nodal officers, technology teams and authorised data recipients involved in data sharing. Such activities shall cover data classification, lawful basis for sharing, consent and beneficiary rights, anonymisation and de-identification, cyber security, privacy safeguards, Data Sharing Agreements, grievance handling, breach reporting, audit logging and responsible use of AI / ML.

The concerned CDO / nodal officer shall also ensure clear internal communication of roles, responsibilities, approval workflows and escalation mechanisms under this Framework. Where data sharing affects beneficiaries or citizens, appropriate communication shall be made in simple and accessible language regarding the purpose of data sharing, rights available, grievance mechanism and safeguards adopted, subject to applicable law and security considerations.

3. Different Types of Shareable Datasets of the MDO

There are basically four types of data available for data sharing.

1. Personal Data (of Natural Person)
2. Entity Data (of Company, Organisation, MSME, Start-ups, etc)
3. Bulk Data
4. Anonymised and De-Identified Bulk Data

The **personal data** sharing needs to factor-in consent of the data owner / data principal and as per the provision of the law, DPDP Act, amendment and regulations.

Entity Data needs to factor-in the contract as made permissible and allowed by entities and in accordance with the law.

Bulk Data can be shared within the government (in accordance with the law) while factoring-in encryption and role based access control. This may have personal / non-personal data at individual and/or at entity level.

Anonymised and De-Identified Bulk Data shall be shared only under an agreement binding the Data Requestor not to use any technique to convert anonymised data into identifiable data, whether by combining it with other data or by applying any algorithm.

4. Different Modes of the Data Sharing

Data under this framework may be shared only through approved, secure and auditable modes, based on the category of data, purpose of sharing, nature of recipient, volume of data requested and applicable legal / security requirements. The default mode for sharing identifiable or restricted data shall be secure API-based access, with bulk sharing permitted only in exceptional cases and subject to specific approval, encryption, access control and audit logging.

The following modes may be adopted:

(A) Modes of Data Sharing based on online and quantum of data

i. **API-based Sharing:** Data may be shared through secure APIs or approved national API gateways for real-time, purpose-bound and system-to-system access. API access shall be role-based, authenticated, time-bound, logged and restricted to approved data fields only. API Setu Platform should be used as an API based data exchange platform.

ii. **Bulk Data Sharing:** Bulk data sharing shall be avoided for personal or high-risk data and may be permitted only where the approved purpose cannot be achieved through APIs, dashboards or query-based access. Any permitted bulk sharing shall be encrypted, password-protected, time-bound, minimised, logged and governed by a Data Sharing Agreement.

iii. **Offline / Exceptional Sharing:** Offline sharing through removable media, email or physical transfer shall be discouraged and may be allowed only in exceptional circumstances with written approval of the CDO / Nodal Officer / competent authority, encryption, secure transfer protocol, recipient acknowledgement and complete audit trail.

(B) Modes of Data Sharing based on digital mechanism

i. Portal / Login-based Sharing: Authorised users may access approved datasets through secure portals using role-based access, strong authentication and user-specific permissions. Such access shall be limited to the approved purpose and shall be subject to monitoring and periodic review.

ii. Consent-based Digital Sharing: Where data relates to a beneficiary / data principal and consent is required, sharing may be enabled through approved consent-based digital channels, such as DigiLocker, Entity Locker or other authorised consent management mechanisms.

iii. Open Data / Public Dashboard Sharing: Fully anonymised, aggregated or non-personal datasets may be shared through open data portals, public dashboards or approved data platforms, subject to re-identification risk assessment and publication approval.

iv. Secure Research / Analytics Access: For research, policy analysis, innovation or AI / ML use cases, data may be made available through controlled environments, data sandboxes, secure data enclaves or approved analytical platforms, with restrictions on download, re-identification, onward sharing and publication of outputs (Reference Option 2 under Section 2.3, Part C, item 2 - Anonymisation and De-Identification for Bulk Data). AI Kosh should be used as a data exchange platform. Other Government initiatives and domain-specific data repositories, such as the Indian Biological Data Centre and the ICMR Health Research Data Repository, among others can also be used.

5. Data Sharing Requisite

5.1. Data Classification Framework

All datasets held by the MDO may be classified into one of four categories. The classification governs who may access the data, what approval is required, and through which platform it is shared.

Category	Definition	Examples	Example of Mode of Data Access	Platform
Open Access (CAT-1)	Fully anonymised, aggregated, or non-personal data. No risk of re-identification.	Aggregate statistics, counts, district-level summaries, reference data.	Open — no login required	data.gov.in (OGD), API Setu, NDAP, AI-Kosh, eSankhyiki
Registered Access (CAT-2)	De-identified data useful to researchers, start-ups, and civil society. Individual identity not exposed.	Anonymised scheme data, de-identified health datasets, economic statistics.	Login / KYC + purpose declaration	API Setu, NDAP, AI-Kosh, OGD, Microdata, Ministry portals
Restricted Access (CAT-3)	Personal or sensitive data at individual or entity level. Shared only with DPDPA-compliant consent or specific legal mandate.	Vehicle / DL records, Aadhaar-linked records, individual scheme benefits.	API-based, purpose-bound, annual renewal	API Setu, NAPIX, DigiLocker, Entity Locker
Non-Shareable (CAT-4)	Classified, national-security-sensitive, or legally restricted data.	Intelligence records, Cabinet deliberations, strategic infrastructure data.	Not shared externally	Internal government network only

Note: Each dataset should be detailed out in terms of machine-readable data fields. The original dataset may contain fields which are sensitive. Instead of assigning a single classification to the entire dataset, individual fields or logical groups of fields may be classified according to the potential risk of disclosure, re-identification or misuse. This would facilitate greater data sharing and utility while ensuring that sensitive fields remain appropriately protected.

For example: a beneficiary database with identifiers such as Aadhaar, mobile number and bank account details may be CAT-3. However, after removing these sensitive fields, the beneficiary level remaining data can be a CAT-2 dataset. Further, the aggregated geographic and scheme-related fields like total number of beneficiaries, total expenditure, etc. along with the geographic identifiers may be shared as a CAT-1 dataset.

The synthetic dataset is not covered explicitly as a part of above data classification. The Ministry / Department /Organisation (MDO) may choose to mark the synthetic data as Cat-1, 2, 3 or 4 depending on the metadata and are encouraged to adopt data sharing accordingly.

5.1.1 Classification Register

Every dataset recorded in the Dataset Inventory Register (Section 5.2) must be assigned a category. The Nodal Officer or CDO approves all classifications, which are reviewed annually and published on the MDO's data portal. When in doubt, the higher (more restrictive) category applies.

5.1.2 Example - Dataset having Personal Information (Indicative)

(a) **Dataset along with fields:** Personal Information

- Name
- Name of relative (i.e., s/o, d/o, w/o)
- Date of Birth

- Gender
- Residential Address
- Mobile Number
- Email Address

(b) **Category of dataset:** CAT-3 Restricted Access

(c) **Rationale:** The dataset contains personal data at individual level

(d) **Suggested Mode of Access:** Data Exchange Platform having consent manager like DigiLocker

5.2. Dataset Inventory Register

The Chief Data Officer / Authorised Government Officer in MDO shall maintain a live Dataset Inventory Register covering all databases and applications owned or managed by this MDO. The register must include, at a minimum, the fields below.

S. No.	Source of Dataset	DB / Application	Description	Custodian Division	Tech Host	Approx. Volume	Classification Open Access (CAT-1)/ Registered Access (CAT-2)/ Restricted Access (CAT-3)/ Non-Shareable (CAT-4)	API Available?
1	Scheme Name (1)						CAT-[ ]	[ ] Y [ ] N
2	Scheme Name (n)						CAT-[ ]	[ ] Y [ ] N
3	Service Delivery Portal (1)						CAT-[ ]	[ ] Y [ ] N
4	Service Delivery Portal (n)						CAT-[ ]	[ ] Y [ ] N
5	Survey (n)						CAT-[ ]	[ ] Y [ ] N
6	Regulatory Work						CAT-[ ]	[ ] Y [ ] N
7	Others						CAT-[ ]	[ ] Y [ ] N

* In case, a dataset has data fields pertaining to more than one category then data classification should be done at data field or a set of data field level, which can be made available to be shared.

* Additional fields in the column could be 'Applicable retention period' and 'Date of last classification review'.

Every datasets available for sharing in the Dataset Inventory Register should be made available on the portal of the respective Ministry/ Department/ Organisation (MDO), so that any potential data user can see which data sets and data fields are available for sharing.

Every dataset needs to be accompanied by standardised metadata sufficient to enable discovery, interpretation, assessment and appropriate use of the data. The metadata shall describe the source, ownership, purpose, concepts and definitions, unit of observation, each data field, classifications, coverage, reference period, frequency, methodology, update and revision policy, access category, known limitations and contact points to get the data. The metadata information may also be added in the Dataset Inventory Register for each dataset.

5.3. Data Sharing Platforms

Data sharing mechanism should use the data exchange platform. Ministry / Department / Government organisation can make use of already operational data exchange platforms, alternatively, MDO may develop a data exchange platform of its own and use the same for data sharing. Legacy systems unable to connect natively must expose data via NeGD/NIC-approved API wrappers aligned with the Open API Policy (2015), MDDS standards (egovstandards.gov.in) and National Metadata (NMDS 2.0) Structure. Some of the operational, national level, data exchange platforms are as follows:-

Platform	Open Access (CAT-1)	Registered Access (CAT-2)	Restricted Access (CAT-3)	Non-Shareable (CAT-4)	Indicative Use
API Setu / NAPIX	✓	✓	✓	✗	Primary API gateway for all G2G and G2B sharing. Mandatory for CAT-3 individual record fetch.
DigiLocker / Entity Locker	✗	✗	✓	✗	Citizen and business-facing, consent-based document sharing.
OGD - data.gov.in	✓	✓	✗	✗	Foundational open data portal under NDSAP 2012. For CAT-1 and de-identified CAT-2.
NDAP	✓	✓	✗	✗	Cross-ministry standardised datasets for policy analytics and district-level indicators.
AI Kosh	✓	✓	✗	✗	De-identified, consent-cleared datasets for training AI models. Differential privacy preferred.
Account Aggregator (AA)	✗	✗	✓	✗	Consent-based financial data sharing. Applicable to Finance / DFS datasets.
eSankhyiki	✓	✗	✗	✗	Dissemination of datasets of official statistics
Micro Data Portal	✗	✓	✗	✗	Sharing unit-level anonymised datasets with registered users

5.4. Data Sharing Governance and Approval Process

5.4.1 Data Governance Committee

MDO will set-up the Data Governance Committee. The composition of DGC can be as follows:-

1. Joint Secretary looking after the IT of the MDO / Senior Government Officer of MDO, as nominated by Secretary
2. Scheme Owners (Director of the Division)
3. Representation of Data Exchange Platform or Data Sharing Portal
4. Any other officer as may be nominated by the Secretary

The key responsibility of DGC will be as follows:

1. **Policy ownership and approval of data-sharing requests** - review and update the data-sharing framework / procedure, and act as the designated authority for classification of datasets and monitor the operationalisation of delegated power to approve or reject requests for access to data; also responsible for oversight of data harmonisation initiatives of MoSPI and also the work of Data & Strategy Units.
2. **Compliance and audit oversight** - ensure processing stays within the DPDP Act and other applicable laws; commission periodic audits of the organisation and its ecosystem partners/vendors and verify the usage of data and purpose limitation
3. **Risk management** - maintain a data-sharing risk register with mitigation plans, oversee due-diligence before onboarding third parties, and review residual risks periodically.
4. **Security safeguards and data-breach response** - set technical/organisational security standards, and investigate, adjudicate and track data-breach or cyber-incidents to closure, including statutory notifications to the Data Protection Board, CERT-In, and affected data principals.
5. **Grievance redressal and awareness** - oversee handling of data-principal requests and complaints, and ensure training, awareness and confidentiality undertakings across staff and partners.

5.4.2 Approval Process for Access to Datasets

All data sharing requests must follow the approval matrix below. The process is end-to-end online. Silence is not approval for Category 2 and above.

Category	Approving Officer	Data Type / Access	Timeline	Format
Open Access (CAT-1)	Platform Access (automated)	Open data; **Exempt / Auto**	Instant	Open access; no form
	Platform Access (automated for govt requester)	Data sharing within government; **Automated**	Instant for govt requester	
Registered Access (CAT-2)	Platform Access (Approval by Director for non-govt requester)	Data sharing outside government; **Approval required** (One time registration and multiple time access provision)	<x> working days for approval	Email on standard template; Entry in Data Access Register
Restricted Access (CAT-3)	Joint Secretary / Secretary to GoI	Data sharing within government or outside government; **Approval required**	<y> working days	Annexure III and IV/V form + DPO undertaking + security self-declaration + CERT-In audit + full DSA + DPO certificate

5.4.3 Pre-requisite for sharing data with Data Requestor / Data Recipient

(1) For Open Access (Cat-1) level dataset

Nil requirement

(2) For Registered Access (Cat-2) level dataset

(a) Cat-2 data sharing between Government entities

The Government entity seeking access shall be registered/authenticated on the designated Data Exchange Platform. The access request shall be submitted through the platform by an authorised user/system of the requesting organisation using a duly authenticated and domain-verified official .gov.in / .nic.in email ID or other approved Government authentication mechanism. Upon successful authentication/registration and validation of the access request, the data may be shared through the designated Data Exchange Platform.

(b) *Cat-2 data sharing with non-Government entities*

Private individuals and organisations like start-ups, educational institutions, universities, researchers, research organisations, civil society organisations, NGOs, PSUs, PSBs and other eligible non-Government entities seeking access to Category-2 datasets shall complete registration on the designated Data Exchange Platform / Data Sharing Portal. The applicant shall be authenticated through a simple digital process to verify identity of the individual (if it is human individual request) and/or organisational verification mechanism (if the request is from an organization) and shall provide the details, as required, at the time of authentication.

(3) For Restricted Access (Cat-3) and above level datasets

(a) **Central Ministries, Departments and Organisations -** The request for data access should be made by a Joint Secretary, equivalent or above level officer in his/her letter head. The email ID should be checked with .gov.in or .nic.in domain.
(b) **States and Union Territories -** The request for data access should be made by a Secretary of the department, equivalent or above level officer in his/her letter head. The email ID should be checked with .gov.in or .nic.in domain.
(c) **Private Sector, Start-ups, Academia, Research Organisation, PSUs and PSBs -** The request for data access should be made on the letter head by the authorised representative of the entity, as passed by the Board Resolution. The email ID should be checked with the domain concerned. The entity needs to be registered and headquartered in India. The formal contract between the MDO (data controller / fiduciary) and a recipient specifying purpose, permitted use, security obligations, and deletion terms. (**Annexure III / IV and V**)
(d) **Citizens** - The data request should be made through an electronic consent manager, recognised by the Government of India (e.g. Meri PehChaan, DigiLocker SSO, Parichay, e-Pramaan, or Departmental SSO).

5.4.4 Application form for Data Requestor / Data Recipient

(1) For Registered Access (Cat-2) level data sharing

(a) **Cat-2 data sharing between Government entities**

For Category-2 Government-to-Government access, the request shall be submitted electronically through the designated Data Exchange Platform at the time of authentication for the first time. A separate offline application or physical communication shall not ordinarily be required. Where the requesting organisation is already registered/authenticated subsequent access shall be processed through the platform without requiring submission of a fresh application.

(b) **Cat-2 data sharing with non-Government entities**

Once the applicant is registered and authorised for specified datasets and purposes, access shall be provided through the designated Data Exchange Platform / Data Sharing Portal. The registered applicant shall submit the prescribed application specifying the intended purpose/use case and the datasets required, together with the applicable Data Sharing Agreement/Undertaking. Fresh approval or modification of the existing authorisation shall only be required where the applicant seeks access to additional datasets outside the approved scope, proposes a new or materially different purpose, changes the mode of access, or where the registration / authorisation expires or the risk profile materially changes.

(2) For restricted Access (Cat-3) and above level, the requesting organisation must submit a standard offline / online Data Sharing Request Form.

(a) Central Ministries, Departments and Organisations (MDO), States and Union Territories

As per Annexure III (application form).

(b) Private Sector, Start-ups, Academia, Research Organisation

Annexure III (application form), Annexure IV (Memorandum of Data Compliances) and Annexure V (Data Sharing Agreement).

(c) Citizens

As per the electronic consent form.

5.4.5 Terms of data usage and data sharing agreement

All shareable datasets shall be accompanied by clearly specified terms of reuse, appropriate to their classification, nature and mode of access.

(1) For open-access (Cat-1 level) datasets

The applicable open-data license shall be prominently indicated on the dataset landing page and, wherever feasible, represented as machine-readable metadata. This shall clearly specify that the Datasets may be copied, redistributed, remixed, transformed and built upon for any purpose, including commercial purposes, subject to the attribution. For example, the standard can be "Government Open Data License (GODL) – India", "Creative Commons Attribution 4.0 International License, written as CC by 4.0" or as find appropriate by MDO.

(2) For Registered Data (Cat-2 level) sharing between Government entities

Category-2 Government-to-Government data sharing shall be governed by the applicable terms of use, security requirements, purpose limitation and access conditions prescribed by the data providing organization and captured through the Data Exchange Platform.

A Data Sharing Agreement or standing data-sharing protocol may be adopted, if required by the data providing organization, based on the nature or risk of the dataset or applicable legal/statutory requirements. Execution of separate Data Sharing Agreement shall not be a mandatory pre-condition for every Category-2 Government-to-Government access request.

(3) For Registered Data (Cat-2 level) sharing with non-Government entities

Access to Category-2 datasets by non-Government entities shall be subject to the terms and conditions prescribed by the data providing organization, including purpose limitation, confidentiality, data security, retention and deletion requirements and restrictions on unauthorised disclosure, onward sharing, re-identification or resale.

The Data Recipient shall provide the prescribed Data Sharing Agreement/Undertaking at the stage of initial registration/authorisation and shall remain bound by its terms for the period for which access is authorised.

The Data Sharing Agreement/Undertaking shall not require execution of a fresh agreement for every subsequent access transaction to an already authorised Category-2 dataset, provided the access remains within the approved purpose, scope and validity period.

(4) Every sharing arrangement at **Cat-3** and above must be formalised in a Data Sharing Agreement (DSA) issued by the MDO. MDO may also choose to have a Non-Disclosure Agreement (NDA). The DSA must include, at a minimum, the clauses as below.

Clause	Mandatory Content
Purpose	Data used only for the stated purpose and within the approved duration. Secondary use requires a written amendment. (Basis: DPDPA 2023)
Data fields	Limited to fields specified in Schedule A. No additional fields without written amendment.
De-identification	All bulk data is de-identified before transfer. Individual data shared only via API Setu / DigiLocker with DPDPA-compliant consent.
Security	ISO 27001 or equivalent. Security controls as per Schedule B. Sub-processing prohibited without prior written Ministry consent.
Audit rights	The [MDO], or an auditor appointed by it, may audit the recipient systems on seven (7) days' prior notice. A CERT-In empanelled auditor is required for CAT-3 and above.
Breach notification	Notify the Data Provider's CDO / Nodal Officer without delay and in any event within six (6) hours of becoming aware. Submit a full incident report with root-cause analysis within seventy-two (72) hours. The Data Recipient shall fulfil the obligations as per DPDPA and time-to-time advisories issued by CERT-In.
Deletion	All data is deleted on contract expiry or termination. A deletion certificate or log-based evidence of destruction to be provided within <x days say, 30 days>.
No re-identification or resale	Re-identification, onward sharing, and resale of data are expressly prohibited. Violations attract penalties under DPDPA 2023 and the terms of this agreement.
Governing law	Laws of India; jurisdiction: [for example - New Delhi].

5.4.6 Purpose Code Framework

All CAT-2 and above requests should specify a Purpose Code. The details can be seen at **Annexure III, item (3)** - Purpose Code (Indicative).

5.5. Data Access Charges (Indicative)

The following cost framework is indicative in nature. The monetisation may or may not be considered by MDO.

Data Recipient Type	Data Type	Fee (Indicative)
Individual citizens	Own personal documents / certificates	Free / Chargeable
Government agencies (G2G)	Any shareable category (CAT-1 to CAT-3)	Free / Charge as per agreement between parties
Civil society / NGOs / media / Academic / research institutions / Individuals and Others	CAT-1 - open data	Free via OGD (data.gov.in), NDAP, AI Kosh / Nominal charge as decided by data providers
Civil society / NGOs / media / Academic / research institutions / Individuals and Others	De-identified bulk datasets	Nominal charge (cost recovery and maintenance charge) / Charge as decided by data providers
Regulated private sector (banks, NBFCs, insurers)	CAT-3 API-based individual verification	Transaction-based - Pay per API call (volume slabs)
Commercial / technology companies	Bulk datasets; high-volume API	Commercial pricing

5.6. Grievance and Complaint Redressal

Each Ministry / Department / Government Organisation shall establish a clear, accessible and transparent grievance redressal mechanism for complaints relating to data sharing, processing, disclosure, correction, update, erasure, withdrawal of consent, misuse, unauthorised access or breach of safeguards.

For grievances relating to digital personal data, the mechanism shall operate in accordance with the Digital Personal Data Protection Act, 2023, the rules made thereunder and other applicable laws. The contact details of the Data Protection Officer, where applicable, or the authorised grievance officer / responsible person shall be prominently published on the relevant website, portal or application.

Grievances involving personal data breach, cyber incident, unauthorised disclosure, re-identification, misuse or court-directed masking / redaction / de-indexing shall be treated as priority matters and escalated to the CDO / nodal officer, DPO / grievance officer, CISO, legal division and competent authority, as applicable.

Citizens and stakeholders may raise concerns about data access or use through:

A. Email: _____-[ministry]@gov.in [Suggestive] | Phone: _____
B. Online portal: [Ministry website] > Data Governance > Raise a Grievance [Suggestive]

6. Review

The CDO / Nodal Officer of MDO shall conduct an annual review of this framework, covering:

A. Dataset inventory: Additions, deletions, and reclassifications.
B. Active DSAs: Renewal, expiry, and deletion certificates received.
C. MDDS compliance: Gaps reported to NDGC.
D. API Setu / NAPIX audit logs: Anomalies and purpose violations.
E. DPDPA compliance: Any updates from NDGC or the Data Protection Board incorporated.
F. Monetisation receipts and expenditure (if any): Reconciled and reported.

The concerned CDO / nodal officer shall periodically review audit logs to identify unusual access patterns, excessive data pulls, purpose violations, unauthorised sharing, re-identification attempts, breach indicators or non-compliance with the approved Data Sharing Agreement. Any anomaly or suspected misuse shall be escalated and handled in accordance with the data breach and incident management procedure under this Framework.

The review should be seen and signed off by the Secretary and placed before NDGC for perusal.

Annexure I: Log Record Format

Log Record Format

API audit logs are critical for tracking and recording actions and events related to API usage, ensuring security, compliance, and monitoring. All agencies granted API-based data access are required to maintain detailed logs for every API access. Audit logs shall be protected against unauthorised access, alteration or deletion and shall be retained for a minimum period of <x> years, or for such longer period as may be required under applicable law, audit requirement, investigation, litigation hold or contractual obligation. These logs must be provided by Data Requestor / Data Recipient Entity to MDO either annually or upon request. The prescribed timelines are indicative and may be determined appropriately based on the nature of data, and applicable laws.

Request Timestamp	Request Method	Request URL
Request Headers	Request Body	Response Status Code
Response Headers	Response Body	Response Time
Client IP Address	Server IP Address	User Agent

Annexure II: Techniques for Data Anonymisation

Technique	Description	When to Use	Risk Level
Pseudonymisation	Replace direct identifiers with a reversible token; original linkage held securely by the data custodian.	G2G sharing where re-identification is operationally necessary (e.g. DBT deduplication, fraud detection)	Medium - reversal key must be protected
Tokenisation	Replace PII with a non-reversible session token for that API call.	API Setu real-time authentication; DigiLocker / Entity Locker fetches	Low - if token management is robust
Aggregation	Group-level statistics; minimum cell size of 10 to prevent inference attacks.	OGD / AI Kosh / NDAP open data (CAT-1 & CAT-2); research datasets	Low
Data Masking	Irreversible masking of specific fields (e.g. last 4 digits of Aadhaar, district-level address).	Portal partial-display; research datasets requiring geographic granularity	Low
Differential Privacy	Mathematical noise is added to statistical outputs so individual records cannot be inferred.	High-sensitivity analytical releases on AI Kosh; NDAP national-level statistics	Very Low - gold standard

Note: Pseudonymisation and Data Masking are de-identification techniques. They do not by themselves achieve anonymisation, because the transformation is reversible or the residual data remains linkable. The Aggregation and Differential Privacy, applied to the thresholds, may be treated as achieving anonymisation.

Annexure III: Sample Application Form by Data Requestor

Optional for Category 2. Mandatory for Category 3 and above.

Note: For handling requests from all Data Recipients and approval by MDO, either the existing data exchange platform of GoI will be used or a platform will be developed. It will facilitate Data Recipients to apply online and allow the verifying and approving authorities to carry out the required action online. Until the online application for the request or approval is developed, manual form will be used by the applicant and communicated through eMail.

(1) Application Form for Central MDO, State and UT As Data Requestor

Field	Details to be filled by Applicant
Name of Applicant Organisation	
Named Authorised Govt Officer at applicant (Joint Secretary, equivalent and above level officer in Central MDO / Secretary, equivalent and above level officer in State)	Name: ___ | Designation: ___ | Contact: ___ | Email: ___
Named CDO / Nodal Technical Officer at applicant	Name: ___ | Designation: ___ | Contact: ___ | Email: ___
Purpose Code	PC-0[ ]
Specific use case	Max. 200 words
Dataset(s) requested and category	CAT-[ ] | Dataset name: ___
Mode of data sharing	[API-based] [Portal Login-based Sharing] [Consent-based Digital Sharing] [Bulk Data Sharing] [Secure Research] [Mobile Application-based Access]
Data Exchange Platform to be used	[ ] API (API Setu) [ ] DigiLocker [ ] Entity Locker [ ] AI Kosh. [ ] MDO Portal [ ] Other (Specify)
Volume of queries / records per year	Estimated value
Duration of access required	
Data storage (servers / cloud or Data Centre / IP range / country)	Server IP (Production): _____ Server IP (Development): _____ DC/Cloud Hosting details (in India/outside India): _____
Security audit reference	CERT-In empanelled auditor (mandatory for CAT-3 and above)
Will data be used to train AI / ML models?	[ ] Yes [ ] No
Proposed retention and deletion schedule	
Times for Access Request	First Time / Renewal
Declaration	I confirm the above is accurate and I am authorised to sign this request. Signature: _____ Date: ___

(2) Application Form for Private Sector, Start-ups, Academia, Research Organisation

Field	Details to be filled by Applicant
Name of applicant organisation	
Type of Applicant organisation (Company, Start-up, Academic, Research Institution, etc)	
Registration identifier	CIN / GSTIN / Udyam / Government Office ID
Named Authorised Officer at applicant (authorised by Board Resolution or an equivalent instrument of the entity)	Name: ___ | Designation: ___ | Contact: ___ | Email: ___
Named CDO / Nodal Technical Officer at applicant	Name: ___ | Designation: ___ | Contact: ___ | Email: ___
Purpose Code	PC-0[ ]
Specific use case	Max. 200 words
Dataset(s) requested and category	CAT-[ ] | Dataset name: ___
Mode of data sharing	[API-based] [Portal Login-based Sharing] [Consent-based Digital Sharing] [Bulk Data Sharing] [Secure Research] [Mobile Application-based Access]
Data Exchange Platform to be used	[ ] API (API Setu) [ ] DigiLocker [ ] Entity Locker [ ] AI Kosh [ ] MDO Portal [ ] Other (Specify)
Volume of queries / records per year	Estimate
Duration of access required	
Data storage (servers / cloud or Data Centre / IP range / country)	Server IP (Production): _____ Server IP (Development): _____ DC/Cloud Hosting details (in India/outside India): _____
Security audit reference	CERT-In empanelled auditor (mandatory for CAT-3)
Named DPO at applicant	Name: ___ | Designation: ___ | Contact: ___
Will data be used to train AI / ML models?	[ ] Yes — AI Kosh Data Sharing Agreement required [ ] No
Proposed retention and deletion schedule	
Times for Access Request	First Time / Renewal
Declaration	I confirm the above is accurate and I am authorised to sign this request. Signature: _____ Date: ___

(3) Purpose Code (Indicative)

Code	Category	Sub-Code: Commercial (C) / Non-Commercial (NC) / Both (B) [Indicative]	Permissible Use	Prohibited Use
PC-01	**Identity Verification**	C / NC / B	KYC for financial services, loan origination, insurance, government service delivery	Profiling, surveillance, marketing
PC-02	**Law Enforcement**	NC	Investigation under court order or statutory mandate; accident investigation	Bulk surveillance; commercial use
PC-03	**Research & Policy**	C / NC / B	Academic / statistical / policy research with de-identified data	Commercial product development; re-identification
PC-04	**G2G Service Delivery**	C / NC / B	Cross-ministry service delivery; DBT deduplication; scheme targeting	Sharing with private entities without approval
PC-05	**Ease of Doing Business**	C / NC / B	Business registration, licensing, compliance verification	Profiling individuals without consent
PC-06	**AI / ML Training**	C / NC / B	Training models on AI Kosh with consent-cleared datasets; IndiaAI Mission	Commercial model training for sale; re-identification
PC-07	**Open Data / Statistics**	C / NC / B	Publication on OGD, NDAP, AI Kosh — must be fully anonymised	Re-identification of published data
<Other>	**<Other>**	C / NC / B	<Other>	<Other>

Annexure IV: Sample Memorandum of Data Compliances

(1) Memorandum of Data Compliances (For API data sharing)

I hereby provide this undertaking in connection with "API based <____> data sharing" As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I will keep API credentials, Secret Key etc. confidential and not share them with any third party.
2. I understand that API access is granted only for a specific application/app, and a maximum of four IPs (2 IPs for Production Servers and 2 IPs for Development Servers) of the user system are whitelisted for access.
3. I will tightly bind API access to the approved application (Mobile App/Web Application) through appropriate access control mechanisms such as secret keys, user-id/password authentication, IP whitelisting, a token exchange mechanism, etc., ensuring that no third party can access the service through the application/APP.
4. I will submit a Security Audit Certificate from CERT-IN empanelled security auditor for the application/app for which the required data access is being requested.
5. I will submit a similar Audit certificate to MDO every year at the time of annual renewal. Failure to do so gives MDO the right to discontinue the data sharing service.
6. I undertake that after the data access is operationalised, log records regarding data access particulars shall be maintained in the prescribed format and shall be shared with the MDO annually or on demand, and with the platform operator where the MDO so directs.
7. I undertake to be responsible for the safety and security of the data received through access. If I am transferred, retired, or released, the details of the new incumbent on the official letterhead, duly signed, and stamped, shall be shared with MDO for updating the records.
8. I undertake to use the shared data only for the purpose justified in the request form.
9. I will not disclose, reproduce, sell, distribute, or transfer any shared data or portion of such data to any third party.
10. I undertake not to use, display, or exchange any shared data in any write-up, paper, presentation, discussion forums, or messaging applications without prior approval from MDO.
11. I undertake that all shared data shall be processed and stored on servers or Data Centres residing in India. The data at any point shall not be transferred, processed, or stored on a server outside India.
12. I undertake to develop and maintain strong policies enforcing strong passwords (password management) and the use of multi-factor authentication (MFA).
13. I undertake to always keep up-to-date Operating Systems (OS), robust Cyber-Security systems, including encryption, intrusion detection systems, other application Software, and employee training, to safeguard the systems and data.
14. I undertake that, upon the request of MDO, I will stop using/processing the data accessed through this mode and shall erase any Personal Data as per the Digital Personal Data Protection Act, 2023.
15. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.
16. The Data Recipient or Data Fiduciary shall comply with the applicable law including Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

I have signed and executed this undertaking on this _____ day of _____, 20 at _____. I hereby declare that I have provided this undertaking willingly, without any undue influence or duress, and that the foregoing statement is true and correct. I commit to abiding by and complying with all the terms of this undertaking.

Name of Applicant Organisation: .....

Name of Authorised Government Officer/ Data Recipient or Data Fiduciary: .....

Designation: .....

Department: .....

Mobile number: .....

Office Phone number: .....

Official Email ID: .....

Office Address: .....

Signature: _____

Name: _____

Seal

(2) Memorandum of Data Compliances (For Portal-based data sharing)

I hereby provide this undertaking in connection with "Portal based <____> data sharing" As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Requester/ Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I undertake to keep the Portal credentials confidential and not share them with any third party.
2. I undertake to change the password immediately after receiving it and thereafter, update the password as frequently as possible.
3. I undertake to be responsible for the safety and security of the data received through the Portal access. If I am transferred, retired, or released, the details of the new incumbent on the official letterhead, duly signed, and stamped, shall be shared with MDO for updating the records.
4. I undertake to use the shared data only for the purpose justified in the request form.
5. I will not disclose, reproduce, sell, distribute, or transfer any shared data or portion of such data to any third party.
6. I undertake not to use, display, or exchange any shared data in any write-up, paper, presentation, discussion forums, or messaging applications without prior approval from MDO.
7. I undertake to comply with password policy and guidelines of the portal and use multi-factor authentication (MFA).
8. I undertake to always keep up-to-date Operating Systems (OS), robust Cyber-Security systems, including encryption, intrusion detection systems, other application Software, and employee training, to safeguard the systems and data.
9. I undertake that, upon the request of MDO, I will stop using/processing the data accessed through this mode and shall erase any Personal Data as per the Digital Personal Data Protection Act, 2023.
10. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance with the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.
11. The Data Recipient or Data Fiduciary shall comply with the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

This undertaking has been signed and executed by me on this _____ day of _____, 2026 at _____. I do hereby declare that this undertaking has been given by me of my own volition without any undue influence or duress and that the foregoing statement is true and correct. I undertake to abide by and comply with all the terms of this undertaking.

Name of Applicant Organisation: .....

Name of Authorised Government Officer/ Data Recipient or Data Fiduciary: .....

Designation: .....

Department: .....

Mobile number: .....

Office Phone number: .....

Official Email ID: .....

Office Address: .....

Signature: _____

Name: _____

Seal

(3) Memorandum of Data Compliances (For Bulk data sharing)

I hereby provide this undertaking in connection with "Bulk <____> data sharing" As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Requester/ Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I undertake the responsibility for the safety and security of the bulk data received through a portable hard disk drive or Secured FTP (SFTP) or download link.
2. I commit to using the Shared Bulk Data only for the Purpose/Justification mentioned at the time of data requisition and shall not disclose, reproduce, sell, distribute, or transfer any Shared Data or portion of such data to any third party for any other purpose, without the prior written consent of the MDO.
3. I commit not to use, display, or exchange any Shared Bulk Data in any write-up, paper, presentation, discussion forums, or messaging applications without prior approval from the MDO.
4. I commit that all Shared Bulk Data shall be processed and stored on servers or Data Centres residing in India. The data at any point shall not be transferred, processed, or stored on a server outside India.
5. I commit to always keep up-to-date Operating Systems (OS), robust Cyber-Security systems, including encryption, intrusion detection systems, other application Software, and employee training, to safeguard the systems and data.
6. I commit that, upon the request of MDO, I will stop using/processing the data accessed through this mode and shall erase any personal information as per the Digital Personal Data Protection Act, 2023.
7. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.
8. The Data Recipient or Data Fiduciary shall comply with the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

This undertaking has been signed and executed by me on this _____ day of _____,2026 at _____. I hereby declare that this undertaking has been given by me of my own volition without any undue influence or duress and that the foregoing statement is true and correct. I undertake to abide by and comply with all the terms of this undertaking.

Name of Applicant Organisation: .....

Name of Authorised Government Officer/ Data Recipient or Data Fiduciary:
.....

Designation: .....

Department: .....

Mobile number: .....

Office Phone number: .....

Official Email ID: .....

Office Address: .....

Signature: _____

Name: _____

Seal

(4) Memorandum of Data Compliances (For Citizen sharing)

I hereby provide this undertaking in connection with <____> data sharing. As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Requester/ Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I undertake to keep the Portal credentials confidential and not share them with any third party, (if applicable).
2. I undertake to change the password immediately after receiving it and thereafter, update the password as frequently as possible (if applicable).
3. I undertake to be responsible for the safety and security of the data received.
4. I will not disclose, reproduce, sell, distribute, or transfer any shared data or portion of such data to any third party.
5. I undertake that, upon the request of MDO, I will stop using/processing the data accessed through this mode and shall erase any Personal Data as per the Digital Personal Data Protection Act, 2023.
6. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023.
7. The Data Recipient or Data Fiduciary shall comply with the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

This undertaking has been signed and executed by me on this _____ day of _____, 2026 at _____. I do hereby declare that this undertaking has been given by me of my own volition without any undue influence or duress and that the foregoing statement is true and correct. I undertake to abide by and comply with all the terms of this undertaking.

Signature: _____
Name: _____

Annexure V: Sample Data Sharing Agreement

DATA SHARING AGREEMENT

(Government-to-Government / Government-to-Third-Party Permissioned Data Sharing)

BETWEEN

[NAME OF MINISTRY / DEPARTMENT / GOVERNMENT ORGANISATION]

(the "Data Provider" / Data Fiduciary)

AND

[NAME OF RECIPIENT ENTITY]

(the "Data Recipient")

Agreement Reference No.: _____

Effective Date: _____

THE PARTIES

This Data Sharing Agreement ("Agreement") is made on the Effective Date stated above, by and between:

(1) **[Name of Ministry / Department / Government Organisation]**, a body / department of the Government of [_____], having its office at [address], represented herein by its [designation of authorised signatory] (hereinafter referred to as the **"Data Provider"**, which expression shall, unless repugnant to the context, include its successors and permitted assigns); and

(2) **[Name of Recipient Entity]**, [constituted under / registered as ____], having its registered office at [address], represented herein by its [designation of authorised signatory] (hereinafter referred to as the **"Data Recipient"**, which expression shall, unless repugnant to the context, include its successors and permitted assigns).

The Data Provider and the Data Recipient are hereinafter referred to individually as a "Party" and collectively as the "Parties".

RECITALS (BACKGROUND)

A. The Data Provider, in the course of discharging its governmental functions and delivering services to citizens and businesses, collects, generates, holds and controls certain data, including data held in custody on behalf of the Government.

B. The Data Recipient has been engaged / authorised to carry out the activities described in Schedule 1 (the "Purpose"), the performance of which requires access to certain data held by the Data Provider.

C. The Parties intend that such data be shared in a controlled, lawful, secure and accountable manner, consistent with the principle of "data for public good", while safeguarding the privacy of data principals and the confidentiality and integrity of the data.

D. The Parties intend that the sharing of personal data under this Agreement shall at all times be in adherence to the Digital Personal Data Protection Act, 2023 and the rules made thereunder, and to all other applicable laws.

E. The Parties wish to record the terms governing the sharing, use, protection, retention and deletion of such data.

NOW, THEREFORE, in consideration of the mutual covenants set out below, the Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, unless the context otherwise requires, the following terms shall have the meanings assigned to them below:

"Anonymisation" means the irreversible process of transforming personal data into a form in which a data principal cannot be identified, whether directly or indirectly, even when combined with other information, having regard to factors such as time, cost and available technology.

"Applicable Law" means all statutes, rules, regulations, notifications, orders, guidelines and policies of the Government of India and the relevant State Government in force from time to time, including the Digital Personal Data Protection Act, 2023; the Information Technology Act, 2000 and the rules made thereunder; the Right to Information Act, 2005; and, where relevant, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

"De-identification" means the process by which identifiers are removed from, masked in, or replaced within personal data such that the data, on its own, no longer directly identifies a data principal.

"Data" means the data described in Schedule 1 that the Data Provider makes available to the Data Recipient under this Agreement, in digital or analog form, whether personal or non-personal, static or dynamic.

"Data Principal" means the identified or identifiable natural person to whom personal data relates (also referred to as a data subject).

"Personal Data" means any data about or relating to a natural person who is identifiable, directly or indirectly, by reference to such data, including any inference drawn from such data for the purpose of profiling.

"Sensitive Personal Data" means personal data, including (without limitation) passwords; financial data; health data; official identifiers; biometric and genetic data; data relating to sex life, sexual orientation, transgender or intersex status; caste or tribe; and religious or political belief or affiliation.

"Permitted Personnel" means the named or role-identified personnel of the Data Recipient listed in Schedule 3 who are authorised to access the Data strictly for the Purpose.

"Negative List" means the data declared by the Data Provider as non-shareable, including data exempt from disclosure under sections 8 and 9 of the Right to Information Act, 2005 or restricted under any other Applicable Law.

"Personal Data Breach" means any unauthorised processing, accidental or unlawful disclosure, acquisition, sharing, use, alteration, destruction of, or loss of access to, personal data that compromises its confidentiality, integrity or availability.

"Purpose" means the specific, lawful and limited purpose for which the Data is shared, as described in Schedule 1, and no other purpose.

"Process / Processing" means any operation or set of operations performed on the Data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, use, disclosure, transmission, restriction, erasure or destruction.

1.2 **Interpretation.** Headings are for convenience only and do not affect interpretation. The singular includes the plural and vice versa. A reference to a statute includes any amendment, re-enactment or rules made under it. The Schedules form an integral part of this Agreement. In the event of any conflict between the body of this Agreement and a Schedule, the body shall prevail unless the Schedule expressly states otherwise.

2. PURPOSE AND SCOPE OF SHARING

2.1 The Data Provider agrees to share, and the Data Recipient agrees to receive the Data described in Schedule 1, solely for the Purpose and on the terms of this Agreement.

2.2 The sharing of Data under this Agreement constitutes permissioned access. It does not transfer any ownership in the Data. The Data Provider (and, where applicable, the Government on whose behalf it acts) remains the owner and controller of the Data at all times.

2.3 Where the Purpose can be achieved using anonymised, aggregated or de-identified data, the Data Provider shall share only such data. Personal data or sensitive personal data shall be

shared only where strictly necessary for the Purpose, and then only the minimum identifiable data required (the principle of data minimisation).

2.4 Nothing in this Agreement requires the Data Provider to share any data forming part of the Negative List, or any data the sharing of which would contravene Applicable Law.

3. PERMITTED USE AND RESTRICTIONS

3.1 The Data Recipient shall use the Data only for the Purpose, and only to the extent necessary for the Purpose.

3.2 The Data Recipient shall not, without the prior written approval of the Data Provider:

(a) use the Data, in whole or in part, for any commercial purpose or for any purpose other than the Purpose;

(b) sell, lease, license, publish, disclose, transfer or otherwise make the Data available to any third party;

(c) combine, match or link the Data with any other dataset (whether obtained privately or otherwise) so as to identify, re-identify or profile any data principal;

(d) attempt to reverse-engineer, re-identify or de-anonymise any anonymised, aggregated or de-identified data through processing by any mode(s) as specified in sub-section (x) of Section 2 of the Digital Data Protection Act, 2023;

(e) retain the Data beyond the period permitted under Clause 9; or

(f) transfer or store the Data outside the territory of India.

3.3 Access to the Data shall be restricted to Permitted Personnel on a strict need-to-know basis. The Data Recipient shall ensure that each Permitted Person is bound by written confidentiality and data-protection obligations no less protective than those in this Agreement, and is sensitised and trained in the handling of the Data prior to access.

3.4 Where the Purpose involves research, statistical or advisory output, the Data Recipient shall ensure that no output, report or publication directly or indirectly identifies any data principal, and that outputs are limited to the public-interest objective recorded in Schedule 1, consistent with the "Five Safes" approach (safe projects, safe people, safe settings, safe data and safe outputs).

4. MODE OF SHARING AND TRANSFER

4.1 The Data shall be provided and accessed only through the secure mode specified in Schedule 1, which shall, wherever feasible, be a secured Application Programming Interface (API) or other access-controlled channel approved by the Data Provider. Bulk download or extraction is permitted only to the extent expressly authorised in Schedule 1.

4.2 All Data in transit and at rest shall be encrypted using industry-standard encryption. Credentials and access keys shall be kept confidential, shall not be shared, and shall be rotated and revoked in accordance with the Data Provider's instructions.

4.3 Each Party shall use only such systems and channels for sharing and accessing the Data as comply with the security standards set out in Schedule 2.

5. DATA SECURITY OBLIGATIONS

5.1 The Data Recipient shall implement and maintain appropriate technical and organisational security measures to protect the Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including the measures set out in Schedule 2.

5.2 Any cloud deployment used in connection with the Data shall be hosted only with a cloud service provider empanelled by the Ministry of Electronics and Information Technology (MeitY), or within a Government data centre, and only within India.

5.3 The Data Recipient shall maintain an audit log recording the identity of each person or system that accesses personal data, the date and time of access, and the purpose of access. Such

logs shall be retained for the period specified in Schedule 2 and made available to the Data Provider on request.

5.4 The Data Recipient shall not store the Data on personal devices, removable media or unmanaged systems, and shall ensure that all devices used to access the Data are secured, access-controlled and managed.

5.5 Each Party shall comply with the latest data security, protection and privacy guidelines, frameworks and instructions issued by the Government of India and, where applicable, the relevant State Government, as updated from time to time.

6. CONFIDENTIALITY

6.1 The Data Recipient shall treat the Data as confidential and shall not disclose it to any person except to Permitted Personnel strictly for the Purpose, or as required by Applicable Law (in which case it shall, to the extent legally permitted, give the Data Provider prompt prior written notice).

6.2 The confidentiality obligations in this Agreement shall survive its expiry or termination and shall continue for so long as the relevant Data remains confidential or as required by Applicable Law, whichever is longer.

7. PROTECTION OF PERSONAL DATA

7.1 Where the Data includes personal data, the Parties shall process such data only in accordance with the Digital Personal Data Protection Act, 2023, the rules made thereunder, and all other Applicable Law(s). The Data Provider acts as the data fiduciary; the Data Recipient acts as a data processor / authorised recipient processing personal data on the instructions of, and on behalf of, the Data Provider, solely for the Purpose.

7.2 The Data Recipient shall not determine the purposes or means of processing the personal data beyond the Purpose, and shall act only on the documented instructions of the Data Provider.

7.3 The Data Recipient shall assist the Data Provider, to the extent reasonably required, in responding to requests from data principals and from regulatory or statutory authorities, and in fulfilling the Data Provider's obligations relating to security, breach notification and impact assessment.

7.4 Personal data shall be collected and processed only to the extent necessary for the Purpose. Sensitisation and training shall be carried out for all personnel handling such data.

8. AUDIT, INSPECTION AND COMPLIANCE

8.1 The Data Provider, or an auditor appointed by it, may, on reasonable prior notice (or without notice where a breach is reasonably suspected), audit and inspect the Data Recipient's systems, premises, records and processes to verify compliance with this Agreement.

8.2 The Data Recipient shall cooperate fully with any such audit, provide access to relevant records and personnel, and promptly remediate any non-compliance identified, within the timeframe specified by the Data Provider.

8.3 The Data Recipient shall maintain accurate records of its processing of the Data sufficient to demonstrate compliance with this Agreement.

9. RETENTION, RETURN AND DELETION OF DATA

9.1 The Data Recipient shall retain the Data only for so long as is necessary for the Purpose and, in any event, no longer than the retention period specified in Schedule 1. The Data shall not be retained permanently for any purpose beyond the period permitted under this Agreement.

9.2 Upon the earlier of (i) completion of the Purpose, (ii) expiry of the retention period, or (iii) expiry or termination of this Agreement, the Data Recipient shall, at the Data Provider's option, securely return or irreversibly delete and destroy all copies of the Data (including backups, derivatives and extracts) in its possession or control.

9.3 The Data Recipient shall, within <x days, say thirty (30) days> of such return or destruction, furnish the Data Provider with a written certificate of destruction signed by its authorised signatory.

9.4 Clause 9.2 shall not apply to the extent that retention is required by Applicable Law, in which case the Data shall remain subject to the obligations of this Agreement for as long as it is retained, and shall be used only for the purpose for which retention is required.

10. PERSONAL DATA BREACH AND INCIDENT MANAGEMENT

10.1 The Data Recipient shall notify the Data Provider, without undue delay and in any event within the timeframe specified in Schedule 2, on becoming aware of any Personal Data Breach or any actual or suspected security incident affecting the Data.

10.2 Such notification shall describe, to the extent known, the nature of the breach, the categories and approximate volume of data affected, the likely consequences, and the measures taken or proposed to address it and to mitigate harm.

10.3 The Data Recipient shall take immediate steps to contain and remediate the breach, shall cooperate with the Data Provider in any investigation and in any notification to regulatory authorities or affected data principals required under Applicable Law, and shall not make any public statement concerning the breach without the Data Provider's prior written consent.

11. INTELLECTUAL PROPERTY AND OWNERSHIP

11.1 All right, title and interest in and to the Data shall remain with the Data Provider (or the Government, as applicable). This Agreement grants the Data Recipient only a limited, non-exclusive, non-transferable, revocable right to access and use the Data for the Purpose.

11.2 Ownership of any reports, analyses, modules, templates, dashboards or other deliverables created using the Data shall be as agreed between the Parties in Schedule 1, and any such deliverable shall not contain or disclose personal data except as expressly permitted under this Agreement.

12. LIABILITY AND INDEMNITY

12.1 The Data Recipient shall indemnify and keep indemnified the Data Provider against all losses, damages, costs, penalties and claims arising from any breach by the Data Recipient (or its personnel or sub-contractors) of this Agreement or of Applicable Law in relation to the Data.

12.2 Nothing in this Agreement limits any liability that cannot lawfully be limited, including liability for breach of statutory data-protection obligations.

13. TERM AND TERMINATION

13.1 This Agreement commences on the Effective Date and continues until the completion of the Purpose or the date specified in Schedule 1, unless terminated earlier in accordance with this Clause.

13.2 Either Party may terminate this Agreement by [thirty (30)] days' written notice. The Data Provider may terminate, and/or suspend access to the Data, with immediate effect if the Data Recipient breaches this Agreement, if the Data Provider reasonably suspects a Personal Data Breach, or if continued sharing would contravene Applicable Law.

13.3 Termination shall not affect any rights or obligations that accrued before termination. Clauses relating to confidentiality, return and deletion of Data, audit, liability and indemnity, and governing law shall survive termination.

14. GRIEVANCE REDRESSAL AND DISPUTE RESOLUTION

14.1 Each Party shall designate a nodal officer (named in Schedule 3) responsible for the operation of this Agreement and for receiving and addressing grievances arising under it.

14.2 The Parties shall first attempt to resolve any dispute amicably through their nodal officers and, failing that, through escalation to their respective heads of department. Any unresolved dispute or difference shall be referred to a sole arbitrator for adjudication in terms of the Arbitration and Conciliation Act, 1996 (as amended), having its seat at ____. The language of the arbitration shall be English, and costs shall be shared equally between the parties.

15. GOVERNING LAW AND JURISDICTION

15.1 This Agreement shall be governed by and construed in accordance with the laws of India. The courts at [____] shall have jurisdiction.

16. MISCELLANEOUS

16.1 **Amendments.** Any amendment to this Agreement shall be in writing and signed by the authorised signatories of both Parties.

16.2 **Assignment.** The Data Recipient shall not assign or subcontract any of its rights or obligations under this Agreement without the prior written consent of the Data Provider.

16.3 **Notices.** All notices shall be in writing and sent to the addresses and nodal officers set out in Schedule 3.

16.4 **Severability.** If any provision is held invalid or unenforceable, the remaining provisions shall continue in full force and effect.

16.5 **No waiver.** No failure or delay in exercising any right shall operate as a waiver of that right.

16.6 **Entire agreement.** This Agreement, together with its Schedules, constitutes the entire agreement between the Parties in respect of its subject matter and supersedes all prior understandings relating to it.

16.7 **Force majeure.** Neither Party shall be liable for failure to perform caused by events beyond its reasonable control, provided that obligations relating to the security and confidentiality of the Data shall continue to apply.

16.8 **Counterparts.** This Agreement may be executed in counterparts, including by electronic/digital signature, each of which shall be deemed an original.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorised representatives on the Effective Date.

For and on behalf of the Data Provider	**For and on behalf of the Data Recipient**
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Date: _____	Date: _____
Seal:	Seal:

Witnesses:

1. _____ 2. _____

SCHEDULE 1 – DESCRIPTION OF DATA, PURPOSE AND TERMS

Item	Particulars (to be completed)
Purpose	[State the specific, lawful and limited purpose, e.g. policy making / monitoring / research / value-added service / programme coordination.]
Description of datasets	[List each dataset / data field shared, with its source department and data dictionary reference.]
Nature of data	Personally Identifiable Information: Yes / No Sensitive Personal Data: Yes / No Anonymised: Yes / No Aggregated: Yes / No
Permission authority	[e.g. Data Governance Committee (DGC) or the nodal officer to whom the DGC has delegated approval for this category, as applicable.]
Mode of sharing	[Secured API / access-controlled portal / other approved channel. Specify whether bulk extraction is permitted.]
Retention period	[State the maximum period for which the Data may be retained, after which it must be returned or destroyed under Clause 9.]
Ownership of deliverables	[State ownership of reports, modules, dashboards or templates created using the Data, per Clause 11.2.]
Price/cost (if any)	[Open/free, or as per applicable data pricing policy. State "Nil" if not applicable.]

SCHEDULE 2 – SECURITY AND BREACH-NOTIFICATION REQUIREMENTS

- Encryption of Data in transit and at rest using industry-standard algorithms.
- Role-based access control, strong authentication and the principle of least privilege.
- Hosting only on MeitY-empanelled cloud or within a Government data centre, located in India.
- Audit logging of all access to personal data, retained for [____] years.
- Personal Data Breach notification to the Data Provider within six (6) hours of becoming aware, with a full incident report within seventy-two (72) hours.
- Prohibition on storage on personal devices, removable media or unmanaged systems.
- Compliance with the latest Government of India and State data-security and privacy guidelines.

SCHEDULE 3 – NODAL OFFICERS AND PERMITTED PERSONNEL

Role	Data Provider	Data Recipient
Nodal Officer (name)	_____	_____
Designation	_____	_____
Email / Phone	_____	_____
Address for notices	_____	_____

Permitted Personnel of the Data Recipient authorised to access the Data:

S.No.	Name / Designation / Role	Access level	Confidentiality undertaking signed (Y/N)
1	_____	_____	_____
2	_____	_____	_____
3	_____	_____	_____

— End of Agreement —

List of Abbreviations

The following abbreviations are used in this Model Data Sharing Framework.

Abbreviation	Full Form
AA	Account Aggregator
AI	Artificial Intelligence
API	Application Programming Interface
CAT	Category (data classification category, e.g. CAT-1 to CAT-4)
CDO	Chief Data Officer
CERT-In	Indian Computer Emergency Response Team
CIN	Corporate Identification Number
CISO	Chief Information Security Officer
CoS	Committee of Secretaries
DBT	Direct Benefit Transfer
DFS	Department of Financial Services
DGC	Data Governance Committee
DL	Driving Licence
DPDP Act / DPDPA	Digital Personal Data Protection Act, 2023
DPO	Data Protection Officer
DSA	Data Sharing Agreement
DST	Department of Science and Technology
EDGC	Empowered Data Governance Committee
EODB	Ease of Doing Business
FTP	File Transfer Protocol
GoI	Government of India
GSTIN	Goods and Services Tax Identification Number
ID	Identifier / Identity Document
IP	Internet Protocol (e.g. IP address)
ISO	International Organization for Standardization
IT Act	Information Technology Act, 2000
KYC	Know Your Customer
LGD	Local Government Directory
MDDS	Metadata and Data Standards
MDO	Ministry / Department / Government Organisation
MeitY	Ministry of Electronics and Information Technology
MFA	Multi-Factor Authentication
ML	Machine Learning
MoRTH	Ministry of Road Transport and Highways
MSME	Micro, Small and Medium Enterprises
NAPIX	National API Exchange
NBFC	Non-Banking Financial Company
NDAP	National Data and Analytics Platform
NDGC	National Data Governance Committee
NDSAP	National Data Sharing and Accessibility Policy
NeGD	National e-Governance Division
NGO	Non-Governmental Organisation
NHA	National Health Authority
NIC	National Informatics Centre
OGD	Open Government Data (Platform)
OS	Operating System
PAN	Permanent Account Number
PC	Purpose Code
PII	Personally Identifiable Information
PSB	Public Sector Bank
PSU	Public Sector Undertaking
RTI Act	Right to Information Act, 2005
SFTP	Secure File Transfer Protocol
SSO	Single Sign-On
URL	Uniform Resource Locator
UT	Union Territory