

Operational Guidelines to the Punjab State Data Policy – Part 2

**Guidelines and Implementation
Manual for the Departments
under the Government of Punjab**

March 2022

Contents

| | | |
|-------|--|----|
| 1 | Introduction to the Operational Guidelines | 6 |
| 1.1 | Overview | 6 |
| 1.2 | Objective of the Operational Guidelines | 6 |
| 1.3 | Scope of the Operational Guidelines | 6 |
| 1.4 | Applicability of the Guidelines | 6 |
| 1.5 | Applicability of Part 2 of the Guidelines | 6 |
| 1.6 | Access for Data | 7 |
| 2 | Establishment of Department Level Implementation Authorities | 8 |
| 2.1 | Departmental Data Cell | 8 |
| 2.1.1 | Roles and Responsibilities | 8 |
| 2.1.2 | Departmental Data Officer | 9 |
| 2.1.3 | Data Contributors | 9 |
| 2.2 | Compliance Grid for Establishing Departmental Implementation Authority | 10 |
| 3 | Guidelines for Data Classification | 11 |
| 3.1 | Establishing Departmental Data | 11 |
| 3.1.1 | Establishing the Departmental Data Catalog | 11 |
| 3.1.2 | Process for Data Cataloging | 11 |
| 3.1.3 | Establishing the Departmental MDR | 11 |
| 3.1.4 | Process for creating the MDR | 12 |
| 3.2 | Open Access Data | 12 |
| 3.2.1 | Overview | 12 |
| 3.2.2 | Defining Open Access Data | 13 |
| 3.2.3 | Process for Identification | 13 |
| 3.3 | Personal/Sensitive Personal Data | 15 |
| 3.3.1 | Overview | 15 |
| 3.3.2 | Defining Personal/Sensitive Personal Data | 15 |
| 3.3.3 | Process for Identification of Personal/Sensitive Personal Data | 16 |
| 3.4 | Registered Access Data | 17 |
| 3.4.1 | Overview | 17 |
| 3.4.2 | Defining Registered Access Data | 17 |
| 3.4.3 | Process for Identification of Registered Access Data | 17 |
| 3.5 | Compliance Grid for Data Classification | 18 |
| 4 | Guidelines for Data Governance Framework | 21 |
| 4.1 | Open Access Data Governance Framework | 21 |
| 4.1.1 | Ownership Guidelines | 21 |

| | | |
|-------|--|----|
| 4.1.2 | Collection and Processing Guidelines | 24 |
| 4.2 | Personal/Sensitive Personal Data Governance Framework | 29 |
| 4.2.1 | Scope and Ownership | 29 |
| 4.2.2 | Policy for Privacy and Disclosure of Information | 30 |
| 4.2.3 | Collection and Processing Guidelines | 30 |
| 4.2.4 | Security Guidelines | 33 |
| 4.2.5 | Rights to the Provider of Information | 36 |
| 4.2.6 | Compliance Grid for Personal/Sensitive Personal Data Collection & Processing | 37 |
| 4.3 | Registered Access Data Governance Framework | 40 |
| 4.3.1 | Step 1: Authentication | 41 |
| 4.3.2 | Step 2: Attestation | 41 |
| 4.3.3 | Step 3: Authorization | 41 |
| 4.3.4 | Compliance Grid for Registered Access Data Collection & Processing | 42 |
| 5 | Departmental Management Information System (MIS) Guidelines | 43 |
| 5.1 | Overview | 43 |
| 5.2 | Development of an MIS | 43 |
| 5.3 | Planning for the MIS | 43 |
| 5.3.1 | Organizational Planning | 43 |
| 5.3.2 | Strategy Planning | 43 |
| 5.3.3 | Information Systems Planning | 44 |
| 5.4 | Implementation Guidelines | 45 |
| 5.4.1 | Implementation Plan | 45 |
| 5.4.2 | Organizing the Department | 45 |
| 5.4.3 | Selection and Procurement of Hardware | 45 |
| 5.4.4 | Procurement of Software | 46 |
| 5.4.5 | Creating the Database | 46 |
| 5.4.6 | Training of Users | 46 |
| 5.4.7 | Creating Physical Infrastructure | 46 |
| 5.4.8 | Transition to the New System | 47 |
| 5.5 | MIS Development Approaches | 47 |
| 5.6 | Compliance Grid for Setting up of Departmental MIS Systems | 47 |
| 6 | Departmental Training and Skill Development | 49 |
| 6.1 | Overview | 49 |
| 6.2 | Compliance Grid for Departmental Training & Skill Development | 49 |
| 7 | Business Continuity | 50 |
| 7.1 | Overview | 50 |
| 7.2 | IT Recovery Strategies | 50 |

| | | |
|-------|---|----|
| 7.3 | Data and restoration | 50 |
| 7.4 | Parameters for developing the IT Disaster Recovery Plan | 50 |
| 7.4.1 | Data Backup | 51 |
| 7.5 | Compliance Grid for Establishing a Business Continuity Plan | 51 |

| Sl. No. | Document Name | Version History | Created By | Reviewed By | Approved By | Submitted On |
|----------------|---|------------------------|-------------------|------------------------------------|--------------------|---------------------|
| 1. | Punjab State Data Policy: Operational Guidelines | 01 | KPMG | World Bank | N/A | 16 November 2021 |
| 2. | Punjab State Data Policy: Operational Guidelines (Part 1, 2 & Annexure) | 02 | KPMG | DGRPG | N/A | 02 March 2022 |
| 3. | Punjab State Data Policy: Operational Guidelines (Part 1, 2 & Annexure A, B, C, D, E) | 03 | KPMG | Government of Punjab, J-PAL, Artha | N/A | 23 March 2022 |
| 4. | Punjab State Data Policy: Operational Guidelines (Part 1, 2 & Annexure A, B, C, D, E) | 04 | KPMG | TBA | TBA | 13 June 2022 |

1 Introduction to the Operational Guidelines

1.1 Overview

The Punjab government envisions a digitally empowered state and has formulated a comprehensive Data Policy in the form of the Punjab State Data Policy (PSDP). The PSDP aims to serve as a guiding instrument to promote inclusive development in the state of Punjab. The data policies formulated in PSDP aim to nurture a data-driven culture in the state of Punjab and would lay down a blueprint for a digitally empowered Punjab resulting in improved governance and citizen satisfaction.

PSDP is part of Punjab government's vision to achieve socio-economic development and inclusive growth by optimal utilization of data and technology. Through this policy, the state aims to nurture a data-driven governance ecosystem. Through PSDP, the government reiterates its firm belief that optimal governance decisions can be taken by leveraging the power of data and technology while ensuring citizen privacy and security.

In this context, a streamlined data governance framework is being laid down for the supervision and enforcement of the PSDP.

Formulation of Data Governance Guidelines is imperative as it sets uniform standards and procedures for all state departments, defines rules on collection, processing and management of data while giving utmost importance to laws, citizen privacy, security, and rights.

This Guidelines report would serve as an institutionalized framework for data management and would define clear rules of engagement across all the state departments with respect to data management.

1.2 Objective of the Operational Guidelines

The primary motive of the governance framework is to lay down policies and standards for legal and ethical management of data holdings and to ensure safe data practices. It would also define the principles to identify the people responsible for the enforcement of the framework and aims to define clear delegation of authority and responsibilities.

The framework would help extract value from all the data already held by the state and to be collected in near future, will aim to enable greater data access, shareability and integration at the state level and would play a vital role in increasing overall efficiency and accountability.

1.3 Scope of the Operational Guidelines

This framework applies to all data and information created, generated, collected, and processed using public funds provided by the Government of Punjab, Central Government funds, and international donor organizations, directly or through authorized agencies by various Departments/ Organizations/Agencies and Autonomous bodies of the Punjab State.

1.4 Applicability of the Guidelines

The overall framework must be adopted by all Departments of the Government of Punjab to be fully compliant to the Punjab State Data Policy.

1.5 Applicability of Part 2 of the Guidelines

Part 2 of the Guidelines outline the framework and the implementation of the PSDP within the Departments of the Government of Punjab.

1.6 Access for Data

All personal data held by the government will be governed by collection modalities and access restrictions mentioned in these guidelines, which are in consonance with the PSDP, the Information Technology Act (Privacy Rules) 2011, Information Technology Act 2000 and the Draft Personal Data Protection Bill 2019. All the Open Access Data sets will be available on Punjab Government's branch of the National Open Government Data (OGD) Platform: <https://punjab.data.gov.in>

2 Establishment of Department Level Implementation Authorities

2.1 Departmental Data Cell

Each Department will establish a Departmental Data Cell which will comprise of the Departmental Data Officer and designated Data Contributors within the Department. The size of the cell would vary from Department to Department and would depend on the quantum of datasets to be published. The Departmental Data Cell will be headed by the Departmental Data Officer (DDO) (Refer to Section 2.1.2) and will notify Data Contributors (Refer to Section 2.1.3) within the Department. The Cell is empowered to employ professionals from project management, data analysis, visualization, and programming domains. As defined within the PSDP, the implementation is expected to entail expenditures for both data owners and data managers for data conversion, data refinement, data storage, quality upgradation, etc.

2.1.1 Roles and Responsibilities

| Open Access Data | Personal/Sensitive Personal Data |
|---|--|
| Preparation of Negative List of datasets | Monitoring and enforcing application of the provisions of these guidelines |
| Preparation of a schedule of datasets to be released in next one year | Taking prompt and appropriate action in response to personal data breach in accordance with the provisions of these guidelines |
| Extend Technical Support for Preparation of datasets, conversion of formats etc. | Examination of any data audit reports and taking any action pursuant thereto issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension, or cancellation thereof and maintaining a database of registered data auditors and specifying the qualifications, code of conduct, practical training and functions to be performed by such data auditors |
| Monitor and manage the Open data initiative in their respective Department and ensure quality and correctness of the data | Monitoring cross-border transfer of personal/sensitive personal data being done by the department |
| Work out an open data strategy to promote proactive dissemination of datasets | Reviewing the codes of practice presented within the guidelines in a periodic manner |
| Institutionalize the creation of datasets as part of routine functioning | Promoting awareness and understanding of the risks, rules, safeguards, and rights in respect of protection of personal data amongst the Departments and providers of information |

| | |
|--|---|
| | Monitoring technological developments and commercial practices that may affect protection of personal/sensitive personal data |
| | Promoting measures and undertaking research for innovation in the field of protection of personal/sensitive data |
| | Advising the SDSC and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of these guidelines |
| | Receiving and inquiring complaints under these guidelines |
| | Performing such other functions as may be prescribed |

2.1.2 Departmental Data Officer

2.1.2.1 Nomination

The Administrative Secretary of each Department will appoint a Senior Officer at the level of Joint Director or above to act as the Departmental Data Officer (DDO). The DDO will be responsible for carrying out and supervising the functions of the Departmental Data Cell. The DDO at the time of his/her appointment will have the following minimum qualifications:

- Have held Public Office for at least 5 years either under the Government of India or in the Government of Punjab
- Recent Public Office held must be related to Information Technology

The DDO will hold office for a maximum term of six years from the date on which he/she enters upon his/her office or until he/she attains, the age of sixty-five years. All further regulations under the Punjab Civil Services Code relating to Personnel Appointment will be applicable for this appointment.

2.1.3 Data Contributors

For contribution of the datasets from offices/organization under the Departments (Refer to Section 4.2.3), the Departmental Data Cell will nominate a 3-5 of Data Contributors who would be responsible in contributing the datasets along with their metadata. Each data contributor must contribute the data as per the given metadata format (Refer to Section 4.1.2) which is based on the Dublin Core Standards¹. The contributed datasets would be

¹ The Dublin Core, also known as the Dublin Core Metadata Element Set, is a set of fifteen "core" elements (properties) for describing resources. This fifteen-element Dublin Core has been formally standardized as ISO 15836, ANSI/NISO Z39.85, and IETF RFC 5013. The Dublin Core Metadata Initiative (DCMI), which formulates the Dublin Core, is a project of the Association for Information Science and Technology (ASIS&T), a non-profit organization. The core properties are part of a larger set of DCMI Metadata Terms. "Dublin Core" is also used as an adjective for Dublin Core metadata, a style of metadata that draws on multiple Resource Description Framework (RDF) vocabularies, packaged and constrained in Dublin Core application profiles. These guidelines

approved by Departmental Data Cell and the PSDP PMU (Refer to Operational Guidelines – Part 1, Section 3).

2.1.3.1 Roles and Responsibilities

Data Contributor could be an officer of the Department who would be responsible for his/her unit/division. The responsibilities of the Data Contributor are as follows:

- Responsible for ensuring quality and correctness datasets of his/her unit/division
- Preparing and contributing the catalogs and resources along with the metadata on the State OGD Platform

Additionally, the Departmental Data Cell can also nominate Subject Matter Experts to aid the Cell in dispensing its functions. The qualifications required for this will be the same as required for Subject Matter Experts for the PSDP PMU.

2.2 Compliance Grid for Establishing Departmental Implementation Authority

| Steps to be taken | Creator | Checker | Approver |
|---|--|---------|----------|
| Step 1: Administrative Secretary of each Department to nominate Departmental Data Officer | Administrative Secretaries of Respective Departments | N/A | N/A |
| Step 2: Departmental Data Officer to nominate 3-5 relevant persons as Departmental Data Contributors for Datasets | DDO | N/A | N/A |
| Step 3: Departmental Data Officer to nominate 3-5 support staff (Subject Matter Experts) to act as the Departmental Data Cell and his/her office within the Department | DDO | N/A | N/A |

have emulated the Dublin Core Metadata Element Set to formulate its Metadata Standards, elaborated further in Section 4.1.2

3 Guidelines for Data Classification

3.1 Establishing Departmental Data

Prior to identifying what kind of data is held by a department it is imperative that the whole gamut of data present within the Department is established within a single source point for holistic analysis. To achieve this each Department will need to establish a Data Catalog and Metadata² Repository (MDR) for the Department.

3.1.1 Establishing the Departmental Data Catalog

A Data Catalog can be defined as collection of metadata, combined with data management information, that helps analysts and other data users to find the data that they need, serves as an inventory of available data, and provides information to evaluate fitness data for intended uses.

3.1.2 Process for Data Cataloging

Data Cataloging for a specific Department is to be undertaken on the Data Catalog provided as Annexure to these guidelines. The Catalog developed is tailored to provide a high-level overview of the level of digitization of the Schemes and their currently available technical specifications. The process will be as follows:

Step 1: Departmental Data Cell to designate Data Contributors for each scheme

Step 2: Departmental Data Cell to conduct training session in collaboration with the PSDP PMU on filling of the Data Catalog

Step 3: Data Contributors to collate data on provided format

Step 4: Departmental Data Cell to review Data Catalog and send it back for revision, if required

3.1.3 Establishing the Departmental MDR

A metadata repository is a database created to store metadata. Metadata Repository can be defined as data about the structures that contain data. Metadata may describe the structure of any data, of any subject, stored in any format.

A well-designed metadata repository typically contains data far beyond simple definitions of the various data structures. Typical repositories store dozens to hundreds of separate pieces of information about each data structure.

² Metadata - Metadata is "data that provides information about other data", but not the content of the data, such as the text of a message or the image itself. There are many distinct types of metadata, including:

- **Descriptive metadata** — The descriptive information about a resource. It is used for discovery and identification. It includes elements such as title, abstract, author, and keywords
- **Structural metadata** — Metadata about containers of data and indicates how compound objects are put together, for example, how pages are ordered to form chapters. It describes the types, versions, relationships, and other characteristics of digital materials
- **Administrative metadata** — The information to help manage a resource, like resource type, permissions, and when and how it was created
- **Reference metadata** — The information about the contents and quality of statistical data.
- **Statistical metadata**, also called process data, may describe processes that collect, process, or produce statistical data
- **Legal metadata** — Provides information about the creator, copyright holder, and public licensing, if provided.

Metadata is not strictly bounded to one of these categories, as it can describe a piece of data in many other ways

3.1.4 Process for creating the MDR

MDR for a specific Department is to be undertaken on the MDR provided as Annexure to these guidelines. The Catalog developed is tailored to provide a field-level overview of the of the data elements for each scheme. The process will be as follows:


Step 1: Departmental Data Cell to designate Data Contributors for each scheme

Step 2: Departmental Data Cell to conduct training session in collaboration with the PSDP PMU on filling of the MDR

Step 3: Data Contributors to collate data on provided format

Step 4: Departmental Data Cell to review MDR and send it back for revision, if required

All identification of data types and further classification will only be undertaken after finishing the Data Cataloging and MDR for departments based on the principles laid down in the subsequent sections.

|  Departmental Capabilities Checklist | |
|--|-------|
| <i>Before conducting the Data Cataloging and MDR exercise, the following checklist should be cross-referenced:</i> | |
| — Department Data Officer has been appointed | (Y/N) |
| — Scheme-level Data Contributors have been appointed | (Y/N) |
| — Subject Matter Experts for Departmental Data Cell has been appointed | (Y/N) |
| — Log-In IDs for the State OGD Platform for all relevant personnel has been generated | (Y/N) |
| — PSDP PMU has conducted relevant trainings on filling of said catalogs | (Y/N) |
| — PSDP PMU has shared all relevant formats and training materials with Departmental Data Cells | (Y/N) |

3.2 Open Access Data

3.2.1 Overview

The government through the course of its citizen services delivery collects processes and generates a large amount of data. But a large portion of this data remains inaccessible to citizens, civil society, despite most of this data being deidentified non-sensitive data. This kind of data can be used for social, economic, and developmental purposes.

There is an urgent need to make this data available in an open format to facilitate use, reuse, and redistribute. Such data must be free from any license or any other mechanism of control.

Opening up of government data in open formats would enhance transparency and accountability while encouraging public engagement. The government data in open formats has a huge potential for influencing incremental social change.

The PSDP mandates the state government departments to proactively open up data and is applicable to all entities of the Government of Punjab.

3.2.2 Defining Open Access Data

As defined by the PSDP,

“A dataset is said to be open if anyone is free to use, reuse, and redistribute it. Open data shall be easily accessible in machine-readable formats that are optimized for machine processing.”

This data shall be accessible at a centrally accessible repository along with other websites owned by the government and/or its institutions.

An indicative list of such data would be:

- Data of aggregates
- Processed/Value Added Data, e.g., GDP, per capita income
- Data generated through delivery of government services e.g., literacy rate, infant mortality rate
- Geospatial data

Each department has the authority to use additional identifiers to justify any classification, which will subsequently be ratified by the DGRPG.

Main characteristic feature of such data would be:

Data which contains low impact information wherein the loss of confidentiality, integrity or availability is expected to have none or limited adverse effect on the individuals and the government department who owns the information.

3.2.3 Process for Identification

The PSDP defines and mandates the classification of data, based on sensitivity. Due to the huge amount of data held by government departments, which generally is an admixture of personal and non-personal data it is crucial to lay down the methodology for proper identification of datasets.

Step 1: The first step for identification of open access data, is that each department within the Government of Punjab to prepare its Negative List of datasets.

The Negative List comprises of datasets which are confidential in nature and benefit the security of the state and its subjects in not being open to the public. This list would need to be compiled and sent to the DGRPG within six months from the notification of these guidelines. All other datasets which do not fall under the negative list would be in the Open List.

Step 2: The open datasets would then need to be prioritized into high value datasets and non-high value datasets.

Defined by the European Union (EU) and subsequently Indian National Regulations such as the National Data Sharing and Accessibility Policy 2012 (NDSAP),

“High-value datasets means documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets”

As per the PSDP, within 6 months from the date of notification of these guidelines, all departments must create comprehensive sets of data which will need to be shared and ratified by the DGRPG.

The segregation of High value and Low value datasets will be governed by the following principles:

- **Completeness** - Datasets released by the government should be as complete as possible, reflecting the entirety of what is recorded about a particular subject. Metadata that defines and explains the raw data should be included as well, along with formulas and explanations for how derived data was calculated. The ability of users to understand the scope of information available and examine each data item at the greatest possible level of detail will be the first identifier for ascribing value to the dataset.
- **Primary** - Datasets released by the government should be primary source data. This includes the original information collected by the government, details on how the data was collected and the original source documents recording the collection of the data. Accuracy of data will play a significant role in ascribing value to a dataset.
- **Timeliness** - Datasets released by the government should be available to the public in a timely fashion. Timely accessibility increases the value of any dataset.
- **Ease of Physical and Electronic Access** - Datasets released by the government should be as accessible as possible, accessibility being defined as the ease with which information can be obtained, whether through physical or electronic means.
- **Machine readability** - Information should be stored in widely used file formats that easily lend themselves to machine processing.
- **Non-discrimination** - “Non-discrimination” refers to who can access data and how they must do so. Barriers to use of data can include registration or membership requirements. Another barrier is the use of “walled garden”, which is when only some applications are allowed access to data. At its broadest, non-discriminatory access to data means that any person can access the data at any time without having to identify him/herself or provide any justification for doing so.
- **Use of Commonly Owned Standards** - Commonly owned (or “open”) standards refer to who owns the format in which data is stored.
- **Licensing** - The imposition of “Terms of Service,” attribution requirements, restrictions on dissemination and so on acts as barriers to public use of data. Maximal openness includes clearly labeling public information as a work of the government and available without restrictions on use as part of the public domain.
- **Permanence** - The capability of finding information over time is referred to as permanence. Information released by the government online should be sticky, i.e., It should be available online in archives in perpetuity.

Such government data can be generated through following processes and events:

- Primary Data e.g., Population Census, Education Census, Economic Survey, etc.
- Processed/Value Added Data e.g., Budget, Planning, etc.
- Data Generated through delivery of Government Services e.g., Income Tax Collection, MGNREGS wage distribution etc.

Step 3: The data which are contributed to the state mandated Open Data Platform have to be in the specified open data format only. The data have to be internally processed to ensure that the quality standard is met i.e., accuracy, free from any sort of legal issues, privacy of an individual is maintained and does not compromise with the National security. While prioritizing the release of datasets, each department will publish as many high value datasets as possible.

3.3 Personal/Sensitive Personal Data

3.3.1 Overview

Data has become one of the key resources for generation and delivery of services in the last few decades. A significant part of delivery of services hinge on the idea of organisations (Government and Private) having access to personally identifiable information of beneficiaries or customers. Thus, it is imperative that there needs to be a policy framework to provide for the protection of the privacy of individuals. This framework needs to specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for adjudicating on said purposes.

The Constitution of India considers the right to privacy as a fundamental right, and it is necessary to protect personal data which is an essential facet of informational privacy.

3.3.2 Defining Personal/Sensitive Personal Data

Due to the sensitive nature of personal data, there are existing and upcoming national policy frameworks which any state under the Union of India will need to adhere to. These regulations are namely the Information Technology Act 2000, the Information Technology Act (Privacy Rules) 2011 and the upcoming Personal Data Protection Bill 2019³.

The PSDP defines non-sharable data in the following manner:

“Sensitive personal data and the datasets which are confidential in nature and are in the interest of the country’s security in not opening to the public would fall in the negative list. Data which is explicitly prohibited from being shared as per Section 8 and Section 9 of the Right to Information Act 2005. The RTI Act, 2005, and Right to Privacy judgment 2017 should be taken into consideration while making this list. Few examples of non-shareable data are biometric information, medical records, etc.”

To define the existing national framework, as per the Information Technology Act (Privacy Rules) 2011:

“Personal Data or Information (in case of the PSDP, non-sharable data) means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.”

As per the same regulation,

Sensitive personal data or information such personal information which consists of information relating to:

- Password
- Financial information such as Bank account or credit card or debit card or other payment instrument details
- Physical, physiological, and mental health condition

³ Draft Personal Data Protection Bill 2019 – The PDP 2019 is the proposed Indian Personal Data Protection Regulation. First proposed in 2018, the bill has undergone multiple rounds of industry and expert consultations with significant changes being made based on suggestions received by the Union Government. The final version is currently under review by Parliament of India and is expected to be brought up in the Monsoon Session of Parliament 2022.

- Sexual orientation
- Medical records and history
- Biometric information
- Any detail relating to the above clauses as provided to body corporate for providing service and
- Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

However, the regulation also identifies that any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these guidelines.

In the upcoming framework, the Personal Data Protection Bill 2019 defines personal and sensitive personal data in the following manner:

“Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.”

"Sensitive personal data" means such personal data, which may, reveal, be related to, or constitute:

- Financial data
- Health data
- Official identifier
- Sex life
- Sexual orientation
- Biometric data
- Genetic data
- Transgender status
- Intersex status
- Caste or tribe
- Religious or political belief or affiliation

The PSDP definition does not, in any way, reduce the ambit of personal and sensitive personal data defined by the multiple national level regulations. Furthermore, as stated earlier any definition accepted by the State of Punjab will need to adhere to national level regulations.

3.3.3 Process for Identification of Personal/Sensitive Personal Data

Similar to Open Access Data, a clear methodology for defining Personal/Sensitive-personal/non-sharable data (negative list) for department held data is necessary, as defined below:

Step 1: Cross-reference datasets held by the department with the mentioned data elements which comprise of Personal Data under National and State level regulations. *Due to the MDR format (Please refer to Annexure E) having classification defined, this subsequent cross-*

checking during this process will be done in adherence to the data classification mentioned in the MDR format.

Step 2: Evaluate if remaining data elements or any other features of the dataset can lead to the discovery of identity of any natural person.

Step 3: Determine if the data element or dataset has been notified as open under the Right to Information Act 2005 and the Right to Privacy Judgement 2017.

Step 4: Cross-reference national level requirements, namely the IT Act (Privacy Rules) 2011 and the Draft Personal Data Protection Bill 2019.

Step 5: Notify identified datasets and elements under the Negative List for the Department

3.4 Registered Access Data

3.4.1 Overview

The responsibility of identifying registered access data rests on each department as the kind of data which needs to be safeguarded while being accessible to the research fraternity will depend on a case-to-case basis.

For example, a registration-based data access policy is the “DatabasE of genomic variation and Phenotype in Humans using Ensembl Resources” or “DECIPHER” implemented by the Harvey Cushing/John Hay Whitney Medical Library of Yale University which works with genetic data. For this project, users who have been approved by the project coordinator (a senior physician working at the center depositing the data) are granted registered access to that project data. DECIPHER projects can be linked to form a consortium, allowing intra-consortium sharing.

3.4.2 Defining Registered Access Data

Registered Access Data can be categorized as data which has a higher risk of harm in the case of re-identification during analysis. This kind of data is most often generated while conducting large scale biological research or large-scale government schemes. The following types of data can be regarded as registered access:

- Data based on sensitive health information (e.g., genetic/epidemiological/sexual information of the population)
- Data based on sensitive economic information of individuals (e.g., wealth/assets/institutionalization/taxation/credit information of the population)
- Data based on sensitive sociological/anthropological information (e.g., education/ethnicity/religion/law/conflict information of the population)
- Data based on state/national resources (e.g., minerals/water/forestry/defense information)

This kind of data is generally used for research purposes. This list is indicative, and the departments are allowed to notify new sets of registered access data, as required.

3.4.3 Process for Identification of Registered Access Data

The flowchart for identification of Registered Access Data will be as follows:

Step 1: Identify Open Access and Personal/Sensitive Personal Data within a department

Step 2: Review Open Access and Personal/Sensitive Personal Datasets for identification of datasets which need an additional layer of security without impeding access for research

Step 3: Notify Datasets identified as Registered Access Data with requirement for special registration for access

3.5 Compliance Grid for Data Classification

| Steps to be taken | Creator | Checker | Approver |
|---|------------------------|------------------------|----------|
| Creation of Data Catalog: | | | |
| Step 1: Departmental Data Cell to designate Data Contributors for each scheme | DDO | N/A | N/A |
| Step 2: Departmental Data Cell to conduct training session in collaboration with the PSDP PMU on filling of the Data Catalog | PSDP PMU | Departmental Data Cell | DDO |
| Step 3: Data Contributors to collate data on provided format | Data Contributors | Departmental Data Cell | DDO |
| Step 4: Departmental Data Cell to review Data Catalog and send it back for revision, if required | N/A | Departmental Data Cell | DDO |
| Creation of Metadata Repository: | | | |
| Step 1: Departmental Data Cell to designate Data Contributors for each scheme | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to conduct training session in collaboration with the PSDP PMU on filling of the MDR | Departmental Data Cell | DDO | DDO |
| Step 3: Data Contributors to collate data on provided format | Data Contributors | Departmental Data Cell | DDO |
| Step 4: Departmental Data Cell to review MDR and send it back for revision, if required | DDO | Departmental Data Cell | DDO |
| Identifying Personal/Sensitive Personal Data: | | | |
| Step 1: The Departmental Data Cell to prepare full list of Datasets available with the Department through Data Cataloging | Departmental Data Cell | DDO | DDO |

| | | | |
|---|------------------------|-----|-----|
| <p>Step 2: The Departmental Data Cell to identify datasets with personal/sensitive personal data elements as outlined in the guidelines</p> <ul style="list-style-type: none"> - The Department may also notify additional data elements, as required | Departmental Data Cell | DDO | DDO |
| <p>Step 3: The Departmental Data Cell to cross-reference if identified datasets have been made public under the Right to Information Act 2005 and the Right to Privacy Judgement 2017</p> | Departmental Data Cell | DDO | DDO |
| <p>Step 4: The Departmental Data Cell to cross-reference if any non-identified datasets have any implications under National Level, IT and Security Regulations</p> <ul style="list-style-type: none"> - Namely the IT Act 2000, IT Act (Privacy Rules) 2011, Draft Personal Data Protection Bill 2019, Official Secrets Act 1927 | Departmental Data Cell | DDO | DDO |
| <p>Step 5: The Departmental Data Officer to validate identified datasets or send them back for revision</p> | Departmental Data Cell | DDO | DDO |
| <p>Step 6: Post review the Departmental Data Cell to notify finalized datasets under “Negative List for Respective Department”</p> | Departmental Data Cell | DDO | DDO |
| Identifying Open Access Data: | | | |
| <p>Step 1: Departmental Data Cell to review Data Catalog to identify datasets with Open Access Data elements as mentioned in the guidelines</p> <ul style="list-style-type: none"> - The Department may also notify additional data elements as required | Departmental Data Cell | DDO | DDO |
| <p>Step 2: Post identification, identified Open Access Datasets to be segregated</p> | Departmental Data Cell | DDO | DDO |

| | | | |
|---|------------------------|-----|-----|
| into High-value Datasets and Low-value Datasets as per principles mentioned in the guidelines | | | |
| Step 3: PSDP Data to ensure coherence with Data Standards for Open Data Publication | Departmental Data Cell | DDO | DDO |
| Step 4: Departmental Data officer to validate the identified datasets or send them back for revision | Departmental Data Cell | DDO | DDO |
| Identifying Registered Access Data | | | |
| Step 1: Review Open Access Datasets for identification of semi-sensitive datasets for implementing a Log-In based additional layer of security | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Officer to validate identified datasets or send them back for revision | Departmental Data Cell | DDO | DDO |
| Step 3: Notify Datasets identified as Registered Access Data with requirement of special registration for access | Departmental Data Cell | DDO | DDO |

4 Guidelines for Data Governance Framework

4.1 Open Access Data Governance Framework

4.1.1 Ownership Guidelines

4.1.1.1 Owner of Published Datasets

Overall owner of published open datasets will be the Government of Punjab. Ownership of specific datasets will be assigned to the departments which notified them. However, if the requirement for such dataset comes from outside the State of Punjab, the owner will be the Government of Punjab.

4.1.1.2 Data Formats

The PSDP recommends that when data is published in an open format it must be machine readable. Though there are many formats suitable to different categories of data, based on analysis of data formats prevalent within the Government of Punjab and keeping adherence with established national standards, open data must be published in the following formats:

- CSV (Comma separated Values)
- XLS (Spread sheet- Excel)
- ODS (Open Document Formats for Spreadsheet)
- XML (Extensive Markup Language)
- RDF (Resources Description Framework)
- KML (Keyhole Markup Language used for Maps)
- GML (Geography Markup Language)
- RSS/ATOM (Fast changing data e.g., hourly/daily)

4.1.1.3 State Open Data Platform (punjab.data.gov.in)

The PSDP mandates that all departments within the Government of Punjab notify its open datasets on the state portal of the Open Government Data (OGD) Platform. The OGD Platform India is located at <https://data.gov.in> and has centralized access to resources (datasets/apps) under catalogs published in open format by various government agencies. Each state operates its own state portal. For Punjab the website is managed by the Department of Governance Reforms and Public Grievances (DGRPG) and can be accessed through <https://punjab.data.gov.in>. The platform provides a search and discovery mechanism for instant access to records.

4.1.1.4 State Open Data License

Following the mandate of the NDSAP 2012 that applies to all shareable non-sensitive data available either in digital or analog forms but generated using public funds by various agencies of the Government of India, it is imperative that all users of Open Datasets published by the Government of Punjab are subject to similar conditions to maintain salience. Following is the license of usage of all open data published by the Government of Punjab and its affiliated agencies.

A. Permissible Use of Open Data published by the Government of Punjab

This license provides all users a worldwide, royalty-free, non-exclusive agreement to use, adapt, publish (either in original, or in adapted and/or derivative forms), translate, display, add value, and create derivative works (including products and services), for all lawful commercial and non-commercial purposes, and for the duration of existence of such rights over the data or information released for open access by the Government of Punjab.

However, while using any data published by the Government of Punjab on its State OGD Platform, the following must be adhered to:

B. Terms and Conditions of Use of Open Data published by the Government of Punjab

Attribution - The user must acknowledge the provider, source, and license of data by explicitly publishing the attribution statement, including the DOI (Digital Object Identifier), or the URL (Uniform Resource Locator), or the URI (Uniform Resource Identifier) of the data concerned.

Attribution of Multiple Data - If the user is using multiple data together and/or listing of sources of multiple data is not possible, the user may provide a link to a separate page/list that includes the attribution statements and specific URL/URI of all data used.

Non-endorsement - The user must not indicate or suggest in any manner that the data provider(s) endorses their use and/or the user.

No Warranty - The data provider(s) are not liable for any errors or omissions and will not under any circumstances be liable for any direct, indirect, special, incidental, consequential, or other loss, injury or damage caused by its use or otherwise arising in connection with this license or the data, even if specifically advised of the possibility of such loss, injury, or damage. Under any circumstances, the user may not hold the data provider(s) responsible for:

- Any error, omission, or loss of data
- Any undesirable consequences due to the use of the data as part of an application/product/service (including violation of any prevalent law).

Continuity of Provision - The data provider(s) will strive for continuously updating the data concerned, as new data regarding the same becomes available. The following SoP will be adhered to while updating the datasets:

- At the time of each updation, the State OGD platform will automatically log the updation of the newer dataset, to enable analysis based on specific periods. The Attribution template in Section 4.1.1.4 (C) will be used for this purpose
- Datasets may be updated on an ongoing basis as is left at the discretion of the Departmental Data Cells
- All Departmental Data Cells will conduct surveys on available datasets and request for new datasets for their department every 90 days
- Not datasets shall be deleted from the State OGD Platform once uploaded without prior written approval of the Chief Data Officer, Government of Punjab
- However, the government does not guarantee the continued supply of updated or up-to-date versions of the data and will not be held liable in case the continued supply of updated data is not provided

C. Template for Attribution Statement

In consonance with the National Open Data License an attribution notice in the following format must be explicitly included:

“[Name of Data Provider], [Year of Publication], [Name of Data], [Name of Data Repository/Website], [Version Number and/or Date of Publication (dd/mm)], [DOI/URL /URI]. Published under [Name of License]: [URL of License].”

For example:

“Planning Department, Government of Punjab, 2018, Annual Building Construction Cost Index from 1981 to 2018, Government of Punjab OGD Platform, 12/20, https://punjab.data.gov.in/catalog/annual-building-construction-cost-index-punjab-1981-2018#web_catalog_tabs_block_10. Published under Punjab State Government Open Data License: [URL of License (this will be the URL of wherever the DGRPG hosts these guidelines)].”

D. Exemptions

The license does not cover the following kinds of data:

- Personal Information
- Data that the data provider(s) is not authorized to license, that is data that is non-shareable and/or sensitive
- Names, crests, logos, and other official symbols of the data provider(s)
- Data subject to other intellectual property rights, including patents, trademarks, and official marks
- Military insignia
- Identity documents
- Any data that should not have been publicly disclosed for the grounds provided under Section 8 of the Right to Information Act, 2005
- The Government from time to time may notify further datasets, upon approval by the State Data Steering Committee

E. Continuity Provision

- Every user of any dataset will endeavor to keep themselves updated on the update history of its publication. The government is not liable for any misrepresentation occurring from usage of dated datasets. However, the government also does not guarantee the continued supply of updated or up-to-date versions of the data and will not be held liable in case the continued supply of updated data is not provided.

F. Breach

- Failure to comply with stipulated terms and conditions will cause the user’s rights under this license to cease automatically
- Where the user’s rights to use data have been ceased under the aforementioned clauses or any other Indian law, these rights will be reinstated only after:
 - Automatically, as of the date the violation is cured, provided it is cured within 30 days of the discovery of the violation
 - Upon express reinstatement by the Government of Punjab
- Upon determination by the Government of Punjab that a specific data set has been published that includes one or multiple kinds of data listed in Section 4.1.1.4(D), the government may terminate the applicability of the license for that data, and this termination will have the effect of revocation of all rights provided under Section

4.1.1.4(A) of this license, including but not limited to immediate retraction of the data set concerned from public access

- For avoidance of doubt, this section does not affect any rights the Government of Punjab may have to seek remedies for violation of this license

4.1.1.5 Compliance Grid for Complying with Open Access Data Ownership Guidelines

| Steps to be taken | Creator | Checker | Approver |
|---|------------------------|---------|----------|
| Step 1: Departmental Data Cell to define usage parameters for each identified Dataset under the Permissible Use Clause of State Open Government Data License for each identified dataset | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to assess terms and conditions and map purpose outliers for each dataset | Departmental Data Cell | DDO | DDO |
| Step 3: Departmental Data Cell to prepare Attribution Template for each identified dataset | Departmental Data Cell | DDO | DDO |
| Step 4: Department to map identified dataset against exemptions mentioned | Departmental Data Cell | DDO | DDO |

4.1.2 Collection and Processing Guidelines

4.1.2.1 Defining Data Contributors

Refer to Section 2.1.3

4.1.2.2 Publishing & Management of Datasets

Contribution of datasets will be a by login-based Dataset Management System (DMS) developed and hosted at <https://punjab.data.gov.in>. Datasets to be contributed will need to ensure compliance with these guidelines. The Departmental Data Cell (Refer to Section 2) notified by Departments are authorized to publish datasets in open format on the State OGD Platform, subject to approval by the PSDP PMU.

Departments have the authority to create any number of Contributors for the contribution of Datasets. Once the Contributor is created, a mail is sent to the mail ID of the contributor. The Contributor then can login and contribute datasets along with its metadata for further approval. However, the responsibility on the relevancy and quality of datasets published on the State OGD Platform rests with the Departmental Data Officer (Refer to Section 2.1.1).

4.1.2.3 Contribution, Approval and Publishing Process for Datasets and Metadata Resources

Step 1: The Departmental Data Officer for open data will Log-In into the State OGD Platform using his/her email-ID provided by the PSDP PMU. Details of the nominated persons and corresponding nomination letters need to be updated within the platform.

Step 2: Nominate Data Contributors. They can be Directors/Joint Directors or Heads of respective divisions/units/schemes. They will coordinate, identify, prepare, and release datasets of their division/unit/scheme.

Step 3: Data Contributors will try to prepare list of datasets which can be contributed. Prepare and contribute the metadata in predefined format for the datasets. The key metadata elements are Title, Description, Sector/Sub-Sector, Dataset Jurisdiction, Keywords, Access

Method, Reference URLs, Data Group Name, Frequency and Policy Compliance. (Refer to Section 4.1.2.7)

Step 4: Datasets along with the metadata contributed by the Data Contributor pass to the Departmental Data Officer, who in turn ensures that it is in compliance with the PSDP and these guidelines. Datasets are published only after such approval.

Step 5: The Departmental Data Officer can edit the datasets or can send it back to the Data Contributor for review/modification or pushes those to PSDP Project Management Unit (PMU) for publishing on the OGD Platform.

Step 6: The PSDP PMU at DGRPG headquarters pushes the datasets/resources from staging module and publishes on OGD Platform.

Additional Requirement: Department in collaboration with the PSDP PMU should organize workshops on the State OGD Platform for Departmental Data Officer, Data Contributors and the Nominated Subject Matter Experts that would help the stakeholders to understand the process better. The PSDP PMU would impart requisite training during the session about how to proceed and optimally make use of the platform for uploading Datasets.

4.1.2.4 Viewing & response to Queries on Published Datasets

The State OGD Portal will provide citizens with functionality like browse, search, filter, sort and access the datasets on the Platform. Citizens will also need to have the option to send their queries and feedbacks about the published datasets. This feedback would be available on the dashboard of each Departmental Data Officer to take further necessary action.

4.1.2.5 Response to Suggestions for new Datasets

The State OGD Platform will also operationalize a citizen suggestions module. Suggestions made for particular datasets will be displayed with a functionality for others to endorse such suggestions. All departments will maintain a list of such suggested lists. These lists are to be sent to the respective department. This would facilitate the Departmental Data Officer to prioritize release of datasets for the platform.

4.1.2.6 Standardization of Data Elements for Data Exchange

Further to collection/contribution of data and prior to publication of the datasets under the prescribed metadata standard for publication (Refer to Section 4.1.2.7).

For data exchange between departments, the PSDP PMU will standardize field level data elements for all datasets identified through Data Cataloging and MDR (Refer to Section 3.1.2 & 3.1.4). These standards will create uniformity between exchanges methodologies between schemes. These field level data standards will be further notified as a sub-policy for these guidelines by the PSDP PMU.



- This will only be possible once the entire Data Catalog and MDR exercise has been completed
- The standards will only be applicable during data exchange
- However, the Departments are urged to store their data as per the notified standards to create coherence between departmental data and improve quality of life
- The PSDP PMU while operationalizing a data exchange will verify these standards and may refuse the request if non-compliance is found
- The PSDP PMU will notify a Compliance Checklist at the time of finalization of these standards for reference

4.1.2.7 Metadata Standards for Dataset Publication

Further to field level data standardization, all datasets will follow the below publication metadata standard for final preparation of the dataset:

Title (Required): A unique name for the catalog (group of resources). For example, Current Population Survey <Year>, Consumer Price Index <Year>, Variety-wise Daily Market Prices Data, State-wise Construction of Deep Tube wells over the years, etc.

Description (Required): Detailed description of the catalog. For example, an abstract determining the nature and purpose of the catalog.

Keywords (Required): It is a list of terms, separated by commas, describing, and indicating at the content of the catalog. Example: rainfall, weather, monthly statistics.

Group Name: This is an optional field to provide a Group Name to multiple catalogs in order to show that they may be presented as a group or a set. For example, 2020-2021 Monthly Weather Data for Punjab.

Sector & Sub-Sector (Required): Choose the sectors(s)/sub-sector(s) those most closely apply to a catalog. For example, Manufacturing, Service, Agriculture (Sector) and Steel Production, Cast Iron Production, Cement production (Sub-sector)

Asset Jurisdiction (Required): This is a required field to identify the exact location or area to which the catalog and resources (dataset/apps) caters to viz. entire country, state/province, district, city, etc.

Frequency (Required): It mentions the time interval over which the dataset is published on the OGD Platform on a regular interval (one-time, annual, hourly, etc.).

Granularity of Data: It mentions the time interval over which the data inside the dataset is collected/ updated on a regular basis (one-time, annual, hourly, etc.).

4.1.2.8 Updation of Datasets

All departments will strive for continuously updating the data concerned, as new data regarding the same becomes available. The following SoP will be adhered to while updating the datasets:

- At the time of each updation, the State OGD platform will automatically log the updation of the newer dataset, to enable analysis based on specific periods. The Attribution template in Section 4.1.1.4 (C) will be used for this purpose along with Publication Metadata Standards (Refer to Section 4.1.2.7)
- Datasets may be updated on an ongoing basis as is left at the discretion of the Departmental Data Cells
- All Departmental Data Cells will conduct surveys on available datasets and requests for new datasets from their department every 30 days
- No dataset shall be deleted from the State OGD Platform once uploaded without prior written approval of the Chief Data Officer, Government of Punjab

| Dos for Data Contribution | Don'ts for Data Contribution |
|--|---|
| Identify and prioritize the release of datasets; categorize the type of access granted for them and publish as many high value datasets as possible. | Don't contribute datasets which fall under the Negative List e.g., the datasets which are confidential in nature and are in the |

| | |
|--|---|
| | interest of the State or the Country 's security. |
| Contribute datasets which are in the Open List and do not fall under the Negative List | Don't impose 'Terms of Service', attribution requirements, restrictions on dissemination and so on, which act as barriers to public use of data |
| Ensure that the quality standards are met i.e., accuracy, free from any sort of legal issues, privacy of an individual is maintained and does not compromise with the National security | Don't impose cost on the public for access of datasets, as imposing fees for access skews the pool of who is willing (or able) to access information. |
| Ensure that the datasets being published through a workflow process are in compliance with these guidelines. Details on original source of the dataset and methodology of the data collection should be provided in metadata | Don't publish handwritten note, as it is very difficult for machines to process. Scanning text via Optical Character Recognition (OCR) results in many matching and formatting errors. Information shared in the widely used PDF format is very difficult for machines to parse. Hence, the data in these formats should be avoided |
| Prepare and contribute the metadata in predefined format. The key metadata elements are Title , Description , Category , Sector/Sub-Sector , Dataset Jurisdiction , Keywords , Access Method , Reference URLs , Data Group Name , Frequency , Granularity of Data and PSDP/Other relevant Policy Compliance . All the metadata elements must be filled with utmost quality and ease of use | Data in non-Unicode formats should be avoided |
| Pricing of data, if any, would be decided by the data owners as per the government policies | Don't contribute datasets with any special characters (e.g., @, %, \$, &, etc.) or missing values. |
| Ensure that data being contributed to the State OGD Platform are in machine readable or in specified open data format only. The advisable formats are: <ul style="list-style-type: none"> • CSV (Comma separated Values) • XLS (spread sheet- Excel) • ODS (Open Document Formats for Spreadsheets) • XML (Extensive Markup Language) • RDF (Resources Description Framework) • KML (Keyhole Markup Language used for Maps) | Don't provide any explanation, including the method of calculation or source of data in data file to be attached in the web form |

| | |
|---|--|
| <ul style="list-style-type: none"> • GML (Geography Markup Language) • RSS/ATOM (Fast changing data e.g., hourly/daily) | |
| Ensure that the data being uploaded on the State OGD Platform is as complete as possible, reflecting the entirety of what is recorded about a particular subject and is de-normalized. The datasets also should be optimized by adding redundant data or by grouping data before uploading. | |
| Priority should be given to data whose utility is time sensitive. Real time information updates would maximize the utility the public can obtain from this information. | |
| Replace any Not Available, Not Reported or missing values in the data with 'NA' | |
| Metadata that defines and explains the raw data should be included as well, along with formulas and explanations for how derived data was calculated | |
| Keywords must be defined in data catalog to make it search friendly | |
| Provide link to the reference documents (if any) or website for detailed information and explanation on the method of calculation or source of data | |

4.1.2.9 Compliance Grid for Open Access Data Collection & Processing

| Steps to be taken | Creator | Checker | Approver |
|---|------------------------|------------------------|----------|
| Collection: | | | |
| Step 1: Define Data Contributors within the Department to sort and consolidate Open Access Datasets | Departmental Data Cell | DDO | DDO |
| Processing: | | | |
| Step 1: Data Contributors to prepare datasets as per prescribed Metadata Standards and prime them for publication on the State Open Government Data Platform | Data Contributors | Departmental Data Cell | DDO |

| | | | |
|---|------------------------|------------------------|-----|
| Step 2: Departmental Data Officer to validate the datasets or send them back for revision | DDO | Departmental Data Cell | DDO |
| Step 3: Departmental Data Officer to ensure adherence to this manual before approving publication of datasets on the State Open Government Data Platform | DDO | N/A | N/A |
| Step 4: Departmental Data Cell to conduct this process once every month to keep datasets updated on the State Open Government Data Platform | Departmental Data Cell | DDO | DDO |
| Publication: | | | |
| Step 1: Departmental Data Cell to prepare datasets following Guideline mandated Open Access Dataset Formats for approved datasets | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to upload finalized datasets on the State Open Government Data Platform Staging Area with Log-In credentials provided by the PSDP PMU | Departmental Data Cell | DDO | DDO |
| Feedback Mechanism: | | | |
| Step 1: Departmental Data Cell to integrate the State Open Government Data Platform Citizen Feedback Module with Departmental PSDP Dashboard | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to integrate State Open Government Data Platform Dataset Suggestion Module with Departmental PSDP Dashboard | Departmental Data Cell | DDO | DDO |

4.2 Personal/Sensitive Personal Data Governance Framework

4.2.1 Scope and Ownership

In addition to open data, these guidelines are being prepared as the implementation roadmap of the PSDP and as such will apply to the:

- The processing of personal data where such data has been collected by the Government of Punjab

- Disclosed, shared, or otherwise processed within the territory of the State of Punjab by the Government of Punjab
- The processing of all personal data and information created, generated, collected, and processed using public funds provided by the Government of Punjab, Central Government funds, and international donor organizations, directly or through authorized agencies by various Departments/Organizations/Agencies and Autonomous bodies of the Punjab State.
- Ownership of personal/sensitive personal datasets will reside with the respective Departments

4.2.2 Policy for Privacy and Disclosure of Information

Any department collecting, receiving, possessing, storing, dealing, or handling information of any provider of information, must clearly produce a privacy policy for handling of or dealing in personal information including sensitive personal data based on these guidelines. This privacy policy must be published on website of the Department. The Privacy Policy will include the following elements:

- Clear and easily accessible statements of its practices
- Type of personal or sensitive personal data or information collected
- Purpose of collection and usage of such information
- Avenues of disclosure of information including sensitive personal data or information
- Security practices and procedures being followed by the Department
- Clear and accessible statements of the rights of the provider of information
- Clear and accessible statements of recourse in case of grievances
- Clear and accessible statements on third parties involved in the processing of said data
- Refer to Annexure A-1 for Format

4.2.3 Collection and Processing Guidelines

4.2.3.1 Collection of Information

The collecting department must obtain consent in writing through letter or fax or email from the provider of the personal/sensitive personal data or information regarding purpose of usage before collection of such information.

Any Department will not collect personal/sensitive personal data or information unless:

- The information is collected for a lawful purpose connected with a function or activity of the Department
- The collection of the personal/sensitive personal data or information is considered necessary for that purpose

While collecting information directly from the person concerned, the Department must ensure that the person concerned is aware of:

- The fact that the information is being collected
- The purpose for which the information is being collected
- The intended recipients of the information

- The name and address of the agency that is collecting the information; and the agency that will retain the information

Any Department holding personal/sensitive personal data or information cannot retain that information for longer than it is required for the purposes for which the information was originally collected or is otherwise required under any other policy/legal requirement for the time being in force.

Personal/sensitive personal information must only be used for the purpose for which it has been collected.

The Department must allow the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

- However, the department will not be responsible for the authenticity of the personal/sensitive personal data or information supplied by the provider of information to the Department or any associated agencies.

The Department prior to the collection of information including sensitive personal data, must provide an option to the provider of the information to not to provide the data or information sought to be collected.

The provider of information, while availing any services being delivered by the collecting Department, will have the option to withdraw its consent given earlier. Such withdrawal of the consent needs to be sent in writing to the department. The Department has the authority to terminate its benefits to the concerned person for whom the said information was denied.

The Department is liable to address any discrepancies and grievances of their provider of the information with respect to details of processing of given information in a time bound manner. For this purpose, the Departmental Data Officer will publish his/her name and contact details on its website. The Departmental Data Officer shall redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.

| Checklist for Collection of Personal Data |
|---|
| 1. Obtain Consent from provider of Information |
| 2. Notify the provider of Information the purpose of collection |
| 3. Notify the provider of Information about intended recipients of the data |
| 4. Notify the provider information about his/her rights |
| 5. Notify the provider of Information of all remedial measures available to him/her in case of any breach |

4.2.3.2 Disclosure of Information

Disclosure of personal/sensitive personal data or information by the department or any associated agencies will require prior permission from the provider of such information, or such disclosure must be agreed to in the contract/agreement between the Department and the provider of information.

In case such disclosure is necessary for compliance of a legal obligation the information shall be shared, without obtaining prior consent from provider of information, with Government

agencies mandated under the law to obtain information including personal/sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government Agency seeking such data will send a request in writing to the Department possessing the personal/sensitive personal data or information clearly stating the purpose of seeking such information. The receiving Government agency must also ensure that the information so obtained shall not be published or shared further.

To promote interoperability and ease of delivery of government services, Departments who wish to access personal/sensitive personal data from other Departments must hold scheme related requirements to justify such transfer through a Standardized Data Exchange Format. (Refer to Operational Guidelines – Part 1, Section 8)

Additionally, the Department on its behalf shall not publish the personal/sensitive personal data or information. Any third parties receiving any personal/sensitive personal data or information from the Department is prohibited from disclosing it further.

| Checklist for Disclosure of Personal Data |
|--|
| 1. Obtain Consent from provider of Information for further disclosure |
| 2. Include such provision in initial consent form, if applicable |
| 3. Justify exchange modalities based on the Standardized Data Exchange Format detailed in these guidelines (Refer to Operational Guidelines – Part 1, Section 8) |
| 4. Ensure personal/sensitive personal data is not published |
| 5. Ensure any third parties receiving such data does not disclose it further without prior consent |

4.2.3.3 Transfer of Information

Any Department may transfer personal or sensitive personal data, to any other Department within the Government of Punjab, that ensures the same level of data protection that is adhered to by the host Department, as provided by these guidelines. The transfer may be allowed only if it is necessary for the delivery of scheme related benefits on its behalf and the provider of information or where such person has consented to data transfer.

4.2.3.4 Personal/Sensitive Personal Data of Children

In case the duties of a department require them to process the personal/sensitive personal data of a child, the Department must process personal data of a child in such manner that protects the rights of, and is in the best interests of, the child.

Any Department shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian.

The manner for verification of the age of child will take into consideration:

- The volume of personal data processed
- The proportion of such personal data likely to be that of child
- Possibility of harm to child arising out of processing of personal data

Due to the sensitive nature of data around children, any department processing significant volumes of data related to children will ensure that no form of profiling, tracking or

behaviorally monitoring of, or targeted advertising is being directed at children. It will also guard against undertaking any other processing of personal data that can cause significant harm to the child. Please refer to Annexure A-3 for format.

4.2.3.5 Processing by entities other than the owner Departments (Authorized agencies by various Departments/Organizations/Agencies and Autonomous bodies of the Punjab State)

In relation to personal/sensitive personal data the owner Department shall not engage, appoint, use, or involve other third-party agencies to process personal data on its behalf without a contract entered into by the owner Department and such party.

The third-party agency shall not engage, appoint, use, or involve another agency in the processing on its behalf, except with the authorization of the Department and unless permitted in the contract entered.

The third-party agency will only process personal/sensitive personal data in accordance with these guidelines and any additional instructions of the Department and treat it as confidential. Please refer to Annexure A-2 for format.

4.2.3.6 Restriction on transfer of Personal/Sensitive personal data outside the State

Personal/sensitive personal data shall only be processed within the State of Punjab. Personal/sensitive personal data may only be transferred outside the state for the purpose of processing, when explicit consent is given by the provider of information for such transfer, and where:

- The transfer is made pursuant to a contract or intra-state scheme approved by the SDSC

Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for:

- Effective protection of the rights of the provider of information in line with these guidelines including in relation to further transfer to any other agency
- Liability of the Department for harm caused due to non-compliance of the provisions of such contract or intra-state scheme by such transfer

The SDSC may allow the transfer of personal/sensitive personal data to another State, or entity or Country, or an international organization on the basis of its finding that:

- Such personal/sensitive personal data shall be subject to an adequate level of protection as provided by these guidelines and extant National Regulations
- Sensitive personal data may be transferred as a copy outside the State, but such sensitive personal data shall continue to reside within the State

4.2.4 Security Guidelines

Every Department must take cognizance of the risks associated with the processing of personal/sensitive personal data and the likelihood and severity of the harm that may result from such processing. Each Department handling personal/sensitive personal data must implement necessary security safeguards, incorporating:

- Methods such as de-identification and encryption (refer to Annexure A-8)
- Steps necessary to protect the integrity of personal data
- Steps necessary to prevent misuse, unauthorised access to, modification disclosure or destruction of personal data

Every Department shall undertake a review of its security safeguards periodically in such manner as may be specified by these guidelines and take appropriate measures accordingly.

4.2.4.1 Reasonable Security Practices and Procedures

The PSDP PMU will notify personal/non-personal data must notify security standards in consonance with the ISO/IEC 27001:2013 Standards⁴, which is mandated by the IT Act (Privacy Rules) 2011, thus governing all data security practices within the Union of India. This standard will be adopted by the departments. The Standard will specify the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the department. This Standard must also include requirements for the assessment and treatment of information security risks tailored to the needs of the department. The requirements set out by the ISO/IEC 27001:2013 standards are generic and are intended to be applicable to all departments within the Government of Punjab, regardless of type, size, or nature. Please refer to Annexure B for the standards manual.

4.2.4.2 Reporting of Personal/Sensitive Personal Data Breach

Every Department by notice shall inform the State Data Steering Committee (SDSC) about any breach of personal/sensitive personal data processed by it where such breach is likely to cause harm to any provider of information.

The notice will include the following particulars:

- Nature of personal data which is the subject-matter of the breach
- Number of data principals affected by the breach
- Possible consequences of the breach
- Action being taken by the Department to remedy the breach

The notice will be made by the Department to the SDSC within 2 working days of the data breach occurring. However, the Department will be allowed up to 5 working days to report the breach given that they have adequate proof to justify that they were adopting any urgent measures to remedy the breach or mitigate any immediate harm.

In case the Department is unsure of any element of the particulars to be included in the notice, the Department shall provide the information to the SDSC in phases without undue delay.

Upon receipt of a notice, the SDSC shall determine whether such breach should be reported by the Department to the provider of information, taking into account the severity of the harm that may be caused to such provider or whether some action is required on the part of the provider to mitigate such harm.

The SDSC may, in addition to requiring the Department to report the personal/sensitive personal data breach to the provider of information, direct the Department to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal/sensitive personal data breach on its website.

The SDSC may, in addition, also post the details of the personal data breach on its website.

⁴ ISO/IEC 27001:2013 - ISO/IEC 27001 is an international standard on management of information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 and then revised in 2013. It details requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure.

4.2.4.3 Data Protection Impact Assessment

Where a Department intends to undertake any processing involving new technologies or large-scale profiling or use of personal/sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to the provider of information, such processing shall not be commenced unless the Department has undertaken a Data Protection Impact Assessment (DPIA) in accordance with these guidelines and has taken approval from the Ethics Committee (Refer to Operational Guidelines – Part 1, Section 5).

The SDSC can further specify circumstances or processing operations where such DPIA shall be mandatory. It will also specify the instances where a Data Auditor will be engaged by the Department to undertake a DPIA.

A DPIA must mandatorily contain:

- Detailed description of the proposed processing operation, the purpose of processing and the nature of personal/sensitive personal data being processed
- Assessment of the potential harm that may be caused to the providers of information whose personal/sensitive personal data is proposed to be processed
- Measures for managing, minimizing, mitigating, or removing such risk of harm

Upon completion of the DPIA, the Departmental Data officer, shall review the assessment and submit the assessment with his/her finding to the Ethics Committee.

On receipt of the assessment and its review, if the Ethics Committee has reason to believe that the processing is likely to cause harm to the providers of information, the Committee may direct the Department to cease such processing or direct that such processing shall be subject to additional conditions as the Ethics Committee may deem fit. Additionally, the Department may hire external consultants to conduct the DPIA.

4.2.4.4 Maintenance of Records

The Department must maintain accurate and up-to-date records of the following:

- Important operations in the data life cycle including collection, transfers, and erasure
- Periodic review of security safeguards and DPIA
- Any other aspect of processing as may be specified by these guidelines

All Departments will provide any provider of information who voluntarily verifies his/her account in relation to the services being received by him/her with a demonstrable and visible mark of verification, which shall be visible to all users of the service.

4.2.4.5 Grievance Redressal

Every Department must have in place the procedure and effective mechanisms to redress the grievances of providers of information efficiently and in a speedy manner.

Any provider of information may make a complaint of contravention of any of the provisions of these guidelines, which has caused or is likely to cause harm to such provider of information, to:

- The Departmental Data Cell
- A complaint made by a provider of information must be resolved by the Department in an expeditious manner and not later than 30 days from the date of receipt of the complaint.

- Where a complaint is not resolved within the period specified or where the provider of information is not satisfied with the manner in which the complaint is resolved, or the Department has rejected the complaint, the provider of information may file a written complaint to the SDSC, to take cognizance of the issue.

4.2.4.6 Offences

Action by any Department which, knowingly or intentionally:

- Re-identifies personal data which has been de-identified without the consent of the SDSC
- Contravenes the provisions made for personal/sensitive personal data by these guidelines

Shall be considered an offence and such case will be presented to the SDSC for adjudication.

Where it has been proved that an offence under guidelines has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Nothing contained in this section shall render any such person liable to any punishment, if he/she proves that the offence was committed without his/her knowledge or that he/she had exercised all due diligence to prevent the commission of such offence.

Where an offence under these Guidelines has been committed by a Department of the State Government or associated agencies, or any authority of the State and it is proved that the offence has been committed with the consent or connivance of or is attributable to any neglect on the part of, any officer, other than the head of the department or authority, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

The provisions of Section 197, Code of Criminal Procedure, 1973 relating to public servants shall apply.

4.2.5 Rights to the Provider of Information

4.2.5.1 Right of Information

The provider of information has the right to know the following information when data is being collected from him/her:

- The purpose and nature of data collection and processing
- The recipient of the data
- The period for which data will be stored
- The identity and contact details of the Highest Notifying Authority for Personal Data for respective departments
- His/her rights in the context of consent withdrawal, and the corresponding procedure
- In case the data will be shared with a third party, details of the third party and rights of consent and withdrawal in such case
- Grievance process, and procedure to approach the grievance officer

4.2.5.2 Right to Correction and Erasure

The provider of information shall where necessary, having regard to the purposes for which personal/sensitive personal data is being processed, have the right to:

- The correction of inaccurate or misleading personal data
- The completion of incomplete personal data
- The updating of personal data that is out-of-date
- The erasure of personal data which is no longer necessary for the purpose for which it was processed

Where the owner department receives a request and the owner department does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such owner department shall provide the provider of information with adequate justification in writing for rejecting the application.

Where the provider of information is not satisfied with the justification provided by the owner department, the provider of information may require that the owner department take reasonable steps to indicate, alongside the relevant personal/sensitive personal data, that the same is disputed by the provider of information.

Where the owner department corrects, completes, updates, or erases any personal data, it shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the provider of information or on decisions made regarding them.

4.2.5.3 Right to be forgotten

The provider of information has the right to erasure of his/her personal data and in such cases, data has to be erased from the system without delay. This Right can be exercised if one of the following applies:

- The personal data is no longer needed in relation to the purpose for which it was collected
- The data subject withdraws his/her consent
- The data subject exercises his/her Right to object
- The personal data has been unlawfully processed/utilized
- The personal data needs to be erased in compliance with law
- The personal data collected is of a child below 16 years of age

4.2.6 Compliance Grid for Personal/Sensitive Personal Data Collection & Processing

| Steps to be taken | Creator | Checker | Approver |
|--|----------|------------------------|----------|
| Collection: | | | |
| Step 1: Establish a Privacy Policy Document (format provided) as a part of the all-scheme related forms, thus ensuring consent for data collection at the ground level | PSDP PMU | Departmental Data Cell | DDO |
| Step 2: Establish a Special Privacy Policy Document (format provided) as part of all-scheme related forms where children are the intended beneficiaries to protect the data of children | PSDP PMU | Departmental Data Cell | DDO |

| Processing: | | | |
|---|------------------------|------------------------|------------------|
| <p>Step 1: PDSP Data Cell to notify reasonable Personal Data Protection Standards for the Department</p> <ul style="list-style-type: none"> - The Personal Data Standards must adhere to the ISO/IEC 27001:2013 Standards as mandated nationally by the IT Act (Privacy Rules) 2011 (Manual provided) | PSDP PMU | Departmental Data Cell | DDO |
| <p>Step 2: For large-scale data processing and processing involving new technologies, the Departmental Data Cell to undertake a Data Protection Impact Assessment (DPIA)</p> | Departmental Data Cell | DDO | Ethics Committee |
| <p>Step 3: Departmental Data Officer the ensure standards before notifying Negative List for the Department or send them back for revision</p> | Departmental Data Cell | DDO | DDO |
| <p>Step 4: Departmental Data Cell to conduct periodic reviews to maintain up to date personal/sensitive personal data and review security safeguards</p> | Departmental Data Cell | DDO | DDO |
| Transferring: | | | |
| <p>Step 1: Departmental Data Cell to adopt Privacy Policy incorporating consent for:</p> <ul style="list-style-type: none"> — Disclosure of Information — Transfer of Information to 3rd Party — Transfer to non-owner Departments — Explicit consent for transfer of Data outside State | Departmental Data Cell | DDO | DDO |
| Reporting in case of Breach: | | | |
| <p>Step 1: Departmental Data Cell to initiate Data Protection Impact Assessment within 24 hours of getting notified of possible data breach of</p> | Departmental Data Cell | DDO | DDO |

| | | | |
|--|------------------------|-----|-----|
| personal/sensitive data and registered access data | | | |
| Step 2: Departmental Data Cell to submit a formal written report to the State Data Steering Committee | Departmental Data Cell | DDO | DDO |
| Step 3: State Data Steering Committee to decide if the breach needs to be notified to affected persons and details published on the State Open Government Data Platform based on parameters mentioned | Departmental Data Cell | DDO | DDO |
| Step 4: Further to the completion of the Data Protection Impact Assessment, the Departmental Data Cell to submit its findings and review of the breach to the SDSC | Departmental Data Cell | DDO | DDO |
| Step 5: The SDSC upon receiving the review may direct the Department to cease such processing or put additional safeguards | SDSC | N/A | N/A |
| Maintenance of Personal/Sensitive Personal Data: | | | |
| Step 1: Departmental Data Cell to formalize record keeping day-to-day usage of personal/sensitive personal data capturing elements mentioned in the Guidelines | Departmental Data Cell | DDO | DDO |
| Step 2: PSDP Cell to conduct Periodic Data Protection Impact Assessments (DPIA) for dataset upkeep, every 8 weeks | Departmental Data Cell | DDO | DDO |
| Step 3: Department to set up verification mark on Scheme MIS, for beneficiaries who have linked all their IDs in relation to any service being provided to them | Departmental Data Cell | DDO | DDO |
| Grievance Redressal: | | | |
| Step 1: Departmental Data Cell operationalize online compliant receiving mechanism within the | Departmental Data Cell | DDO | DDO |

| | | | |
|--|------------------------|-----|-----|
| Department Website along with physical mechanism to receive complaints | | | |
| Step 2: Publish mechanism for lodging complaints and redressal on the Department Website | Departmental Data Cell | DDO | DDO |
| Offences: | | | |
| Step 1: SDSC to officially notify Parameters of Offences mentioned (completed when these guidelines are notified) | SDSC | N/A | N/A |
| Step 2: In case of an offence <ul style="list-style-type: none"> — If the person deemed guilty proves that he/she has was unaware of the breach after successful due diligence on all security provisions of the guidelines, he/she will be exonerated of all charges <p>In case the guilt is proven, the person will be proceeded against under the Code of Criminal Procedure, 1973, provisions relating to public servant</p> | SDSC | N/A | N/A |

4.3 Registered Access Data Governance Framework

Registered Access for data which has been identified for this category must comprise of a three-stage “Triple-A registration” process of Authentication, Attestation, and Authorization. This process aims to ensure both user identification and agreement to a standard set of general responsibilities while considerably simplifying the data access application process.

Through the identification and authentication process, the individual provides “proof” that an asserted identity is their own. The attestation process establishes that the potential data user meets the requirements expected by the consent agreements and ethical approval of datasets in question and includes agreement to comply with the terms of data use required of registered users. Finally, authorization is the overall process by which users are granted access to data and permission to perform specific actions.

The advantage of having a registered access model for certain identified categories of data is to allow access for a relatively large number of authorized individuals thus reducing the administrative burden on departments in managing access to semi-sensitive⁵ datasets. This

⁵ Semi-sensitive Dataset – As explained in Section 3.4.2, departments will notify these datasets which have higher sensitivity than open access data but are not personal or sensitive personal data, thus requiring the added layer of registered access.

model allows broad categories of registered users, such as researchers/professionals to appropriately use such datasets.

4.3.1 Step 1: Authentication

The first step will comprise of the department having datasets relevant for registered access defining the categories of users they would like to allow access. This would comprise of the department gathering information through a process of registration to define user attributes. The attributes requested from users for the registration process, and particularly their verification, will have important implications for access to data protected by registered access authorization methods. Several elements of framework for governance of personal/sensitive personal data have been incorporated within registered access, such as safeguards for disclosure and transfer of information.

Any department applying a registered system must establish a minimal standard (basic registration criteria) which qualifies people who want access as either a bona fide researcher or professional. The standards must include the following details of their identity and research activity:

- Name
- Title
- Position
- Affiliation
- Institutional email address
- Phone number
- Institutional website
- Mailing address
- Purpose for usage of data

This will allow the department to maintain a list of users who has been registered to use the notified datasets, thus covering the authentication part of the “Triple-A” process.

4.3.2 Step 2: Attestation

This step takes influence from the framework for usage and disclosure of personal/sensitive personal data. In this step, the department will verify the authentication details received from requestors of such data with the aim of identifying the purpose for which a notified registered access dataset is required by a researcher/professional.

4.3.3 Step 3: Authorization

The final step will include the department providing access to datasets basis the approval of people whose details have been collected in the first step along with justification of the purpose of usage defined in the second step. The department will decide on who are fit to access registered access datasets. Such review will happen on a case-to-case basis.

4.3.4 Compliance Grid for Registered Access Data Collection & Processing

| Steps to be taken | Creator | Checker | Approver |
|--|------------------------|---------|----------|
| Processing: | | | |
| Step 1: Departmental Data Cell to access module within the State OGD Platform for access to Registered Access Datasets | Departmental Data Cell | DDO | DDO |
| Step 2: Establish Respective Department’s User Authentication Platform within the module to verify users incorporating mentioned elements | Departmental Data Cell | DDO | DDO |
| Step 3: Attest user applications based on purpose for access | Departmental Data Cell | DDO | DDO |
| Step 4: Provide Log-In based Access Mechanism to verified users | Departmental Data Cell | DDO | DDO |
| Publication: | | | |
| Step 1: Departmental Data Cell to prepare datasets following Guideline mandated Open Access Dataset Formats for approved datasets | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to upload finalized datasets on the State OGD Platform Staging Area with Log-In credentials provided by the PSDP PMU | Departmental Data Cell | DDO | DDO |
| Feedback Mechanism: | | | |
| Step 1: Departmental Data Cell to integrate the State OGD Platform Citizen Feedback Module with Departmental PSDP Dashboard | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to integrate State OGD Platform Dataset suggestion with Departmental PSDP Dashboard | Departmental Data Cell | DDO | DDO |

5 Departmental Management Information System (MIS) Guidelines

5.1 Overview

As a part of its Data Consolidation Exercise, every department within the Government of Punjab must implement a Management Information System (MIS) which allows the Department to holistically look at the data that it holds. While a several departments will already have MIS systems in place, it is important to highlight the process of implementing a working MIS system for Departments which are struggling with digitizing their data. All new systems implemented will adhere to the following guidelines.

5.2 Development of an MIS

In MIS, the information is recognized as a major resource like capital and time. If this resource has to be managed well, a department must plan for it and control it, so that the information becomes a vital resource for the system. Key considerations for the department while building an MIS should be:

- The system should deal with the governance/policy planning information not with data processing alone
- It should provide support for the planning, decision-making and action
- It should provide support to the changing needs of the Department

5.3 Planning for the MIS

5.3.1 Organizational Planning

Any MIS design and development process must address the following issues successfully:

- There should be effective communication between the developers and users of the system
- There should be synchronization in understanding of management, processes, and IT among the users as well as the developers
- Understanding of the information needs of Officers from different functional areas and combining these needs into a single integrated system
- The MIS has to interact with the complex environment comprising all other sub-systems in the overall information system of the organization
- It should keep pace with changes in environment, changing demands of the government projects, beneficiaries and future schemes which might be added by the department
- There should not be a need for frequent and major modifications

5.3.2 Strategy Planning

Once the organizational planning stage is over, the Department must take the following strategic decisions for the achievement of MIS goals and objectives:

- Development Strategy, for e.g., an online, real-time batch
- System Development Strategy – Here the Department will select approach to system development like operational versus functional, accounting versus analysis.

- Resources for the Development – The Department will assign resources for the development of the MIS. Resources can be in-house or external
- Manpower Composition – The staff should have analysts, and programmers

5.3.3 Information Systems Planning

The Department as a part of its planning MIS planning will need to undertake Information system planning, which essentially involves:

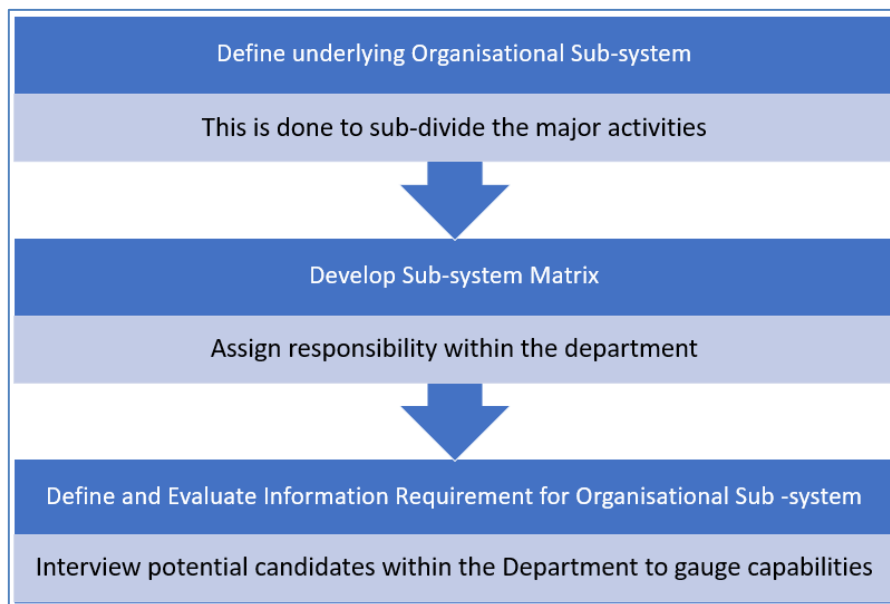
- Identification of the stage of the current information system in the Department
- Identification of the intended usage of the Departmental Information System based on the role of the Department
- Determining the optimum architecture of the Information System for serving the roles identified

The following flowchart outlines the development phase:



5.3.3.1 Information Systems Requirement Analysis

The following diagram illustrates the process of information systems requirement analysis:



The Department must choose from the following three methodologies which can be adopted to determine the requirements in developing an MIS for the Department management information system:

- **Business Systems Planning (BSP)** – This approach identifies the Information System priorities of the organization and focuses on the way data is maintained in the system. It uses data architecture supporting multiple applications and it defines data classes using different matrices to establish relationships among the organization, its processes, and data requirements.

- **Critical Success Factor (CSF)** – This methodology identifies key business goals and strategies of each resource as well as that of the Department. Next, it looks for the critical success factors underlying these goals. Measure of CSF effectiveness becomes an input for defining the information system requirements.
- **End/Means (E/M) analysis** – This methodology determines the effectiveness criteria for outputs and efficiency criteria for the processes generating the outputs. At first it identifies the outputs or services provided by departmental processes, then describes the factors that make these outputs effective for the department. Finally, it selects the information needed to evaluate the effectiveness of outputs.

5.4 Implementation Guidelines

5.4.1 Implementation Plan

The Implementation Plan will consist of the following action-oriented steps:

- Creating a master schedule of the implementation activities
- Setting timelines for critical and non-critical activities
- Identifying major bottlenecks and their solutions
- Communication of the plan

5.4.2 Organizing the Department

While Data will be stored at the State Data Centre under the custodianship of the DGRPG, the Department will be the custodian of the MIS system. The development of the MIS will be carried out by an Implementation body within the Department and will comprise of the following steps:

- Implementation Roles of each member of the department have to be clearly laid out before the new system becomes operational
- Workshops to be conducted to ensure that each role understood by members of the Implementation Body within the Department

5.4.3 Selection and Procurement of Hardware

For the procurement of hardware necessary for the development of the MIS, the following steps will be followed:

- **Preparation of Vendor list** – The Department in consultation with the DGRPG will prepare a list of reliable hardware vendors. This list of vendors may be prepared after analyzing the vendor management experience of the Department with different vendors or may be prepared based on an accepted list of vendors developed by Departments with already operational MIS, ratified by the DGRPG.
- **Preparation of RFP** – Second, the implementation body within the Department must prepare the request for proposal (RFP) document based on their understanding of the hardware requirement of the new system. The RFP must have complete technical details about the required hardware systems including specifications, format, performance expectation, and warranty and service quality requirements⁶. This document is prepared by the implementers in consultation with Department and the DGRPG so that the need for each specification is well established and there is no scope for any difference of

⁶ The RFP requirements will be derived from the governance, security and exchange framework established by these guidelines and ensure interoperability with the State OGD Platform and its components

opinion. The RFP will also have commercial details. Legal advice may be sought prior to notification of the RFP.

- **Request for bids/proposal to select vendors** - After the RFP is prepared it is sent by some mode of communication to the enlisted set of vendors. The communication medium can be an open advertisement in print or electronic media or may be in the form of a letter to the vendors with a deadline for submission of the proposal.
- **Evaluation of RFP** - After bids are received before the deadline, in consultation with the DGRPG, the Implementation Body of the Department will evaluate the proposals. The evaluation may be on the basis of cost alone or quality alone or may be a mix of both cost and quality. Typically, a score-based system of evaluation is used to rank the vendors' proposals. Scores are assigned to each attribute of a vendor's proposal like cost, goodwill, track record and service quality guarantee. Based on the weight age given to each attribute a composite score is prepared, which is used to evaluate the proposals. However, the department must take care to apply the same evaluation criteria to all proposals.
- **Selection of vendor** - Based on the evaluation a single vendor or a select set of vendors are chosen for delivery of hardware. Contract negotiations and price negotiations are held with this select group of vendors and following the successful completion of the negotiations the final contract will be signed.

5.4.4 Procurement of Software

The new system being implemented will have been created based on assumptions of operating environment of the organization. Procurement of system software will be done on similar lines as the procurement of hardware. The only difference in the case of procurement of software is that the choice of what software to purchase is already made at the design stage of the system development and hence, the RFP preparation process is straightforward. The implementation team need not prepare the specification for the system software. They only need to procure the system software that the new system is designed to run on. The rest of the process is almost similar to the hardware procurement process.

5.4.5 Creating the Database

The new system to be implemented will have data stores. These databases are relational database management systems, which is a separate application software package. These databases will maintain interoperability with the State OGD Platform.

5.4.6 Training of Users

The Department will undertake a training needs assessment for its employees, further to which the department will develop a training programme. This is an important part of the implementation process and helps in reducing the resistance to change related behavior among the user community. The training also helps users to appreciate the new features of the new system and helps build trust and appreciation for the new system.

5.4.7 Creating Physical Infrastructure

The new system being implemented may require a physical infrastructure. The implementation team must ensure that the system performance must not suffer due to infrastructure bottlenecks. The Department is mandated to provide for the required physical infrastructure so that it does not affect the performance of the new system.

5.4.8 Transition to the New System

In case the department has a digital system in place, the new system and the old system will both be used for a period to ensure that the Department's performance does not suffer due to transition problems. The old system will be phased out within 6 months from the implementation of the new MIS System.

5.5 MIS Development Approaches

The Government of Punjab will follow a Prototype Model for the Implementation of its MIS Systems. Prototyping is the process of building an experimental system quickly and inexpensively for demonstration and evaluation so that end users can better define information requirements. The prototype is a preliminary model that is refined until it meets end-user requirements. The process of repeating the steps to build a system over and over again is called an iterative process.

The four-step model of the prototyping process consists of the following:

- (1) Identify the Department's basic requirements
- (2) Develop a working prototype
- (3) Use the prototype
- (4) Revise and enhance the prototype.

The process of developing a prototype can be broken down into four steps. Because a prototype can be developed quickly and inexpensively, systems builders can go through several iterations, repeating steps 3 and 4, to refine and enhance the prototype before arriving at the final operational one.

Prototyping is most useful when some uncertainty exists about user requirements or a design solution. It is especially valuable for the design of the end-user interface of an information system such as on-line screens and commands. The intense end-user involvement in prototyping promises the elimination of excess development costs and design flaws that occur when requirements are not fully captured the first time around.

Applications that are oriented to simple data manipulation and records management are considered good candidates for prototyping, but systems based on batch processing or that rely on heavy calculations and complex procedural logic are generally unsuitable for prototyping. Large systems must be subdivided so that prototypes can be built one part at a time.

5.6 Compliance Grid for Setting up of Departmental MIS Systems

| Steps to be taken | Creator | Checker | Approver |
|---|------------------------|---------|----------|
| Step 1: Departmental Data Cell to establish Departmental MIS Organization Plan based on principles mentioned in the Guidelines | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to establish Departmental MIS strategy planned based on principles mentioned in the guidelines | Departmental Data Cell | DDO | DDO |
| Step 3: Departmental Data Cell to review current Departmental Information Systems | Departmental Data Cell | DDO | DDO |

| | | | |
|---|------------------------|-----|-----|
| to establish requirements of the revamped MIS System | | | |
| Step 4: Departmental Data Cell to create a master schedule for all implementation activities | Departmental Data Cell | DDO | DDO |
| Step 5: Departmental Data Cell to prepare list of Hardware and Software vendors in consultation with PSDP PMU | Departmental Data Cell | DDO | DDO |
| Step 6: Request for Proposal to be floated based on identified requirements | Departmental Data Cell | DDO | DDO |
| Step 7: Departmental Data Cell to evaluate bids in consultation with the DGRPG and select Vendor | Departmental Data Cell | DDO | DDO |
| Step 8: MIS Data Storage System to be integrated with the State data Centre | Departmental Data Cell | DDO | DDO |
| Step 9: Departmental Data Cell to create physical infrastructure for implementation based on MIS Development approaches outlined | Departmental Data Cell | DDO | DDO |
| Step 10: Departmental Data Cell to facilitate transfer of all data to new Departmental MIS | Departmental Data Cell | DDO | DDO |
| Step 11: Departmental Data Cell to create Capacity Building Modules for Departmental Employees | Departmental Data Cell | DDO | DDO |
| Step 12: Departmental Data Cell to create Policy Planning Dashboard based on Data Visualization parameters | Departmental Data Cell | DDO | DDO |

6 Departmental Training and Skill Development

6.1 Overview

As mandated in Part 1 of these guidelines, the PSDP PMU will be responsible for the notification of all necessary training modules related to the provisions of the PSDP and its guidelines. Further to the PMU notifying and making the training modules available, the Departmental Data Cells will notify internal training schedules along with making these modules easily available on their Departmental Website.

6.2 Compliance Grid for Departmental Training & Skill Development

| Steps to be taken | Creator | Checker | Approver |
|---|------------------------|---------|----------|
| Step 1: Departmental Data Cell to notify schedule of trainings established by the PSDP PMU | Departmental Data Cell | DDO | DDO |
| Step 2: Departmental Data Cell to prepare internal training schedule based on online training material developed by the PSDP PMU | Departmental Data Cell | DDO | DDO |

7 Business Continuity

7.1 Overview

Through the implementation of the PSDP, the Government of Punjab is trying to create a repository of data vital to the survival and continued operation its services. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. Thus, an information technology disaster recovery plan (IT DRP) must be developed by the PSDP PMU in case of natural disasters.

7.2 IT Recovery Strategies

Recovery strategies should be developed for Information technology (IT) systems, applications, and data. This includes networks, servers, desktops, laptops, wireless devices, data, and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of service functions and its processes. IT resources required to support time-sensitive operations should be given priority.

Information technology systems require hardware, software, data, and connectivity. Without one component of the “system,” the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices, and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)

7.3 Data and restoration

Ideally the Government of Punjab should operate dual data centers capable of handling all data processing needs, which run in parallel with data mirrored or synchronized between the two centers. Due to the State currently having only one such center, the preferable solution is:

- **Vendor Supported Recovery Strategies** - The Government may recruit vendors that can provide “hot sites” for IT disaster recovery. These sites are fully configured data centers with commonly used hardware and software products. Data streams, data security services and applications can be hosted and managed by vendors. This information can be accessed at the primary business site or any alternate site using a web browser. If an outage is detected at the client site by the vendor, the vendor automatically holds data until the client’s system is restored. These vendors can also provide data filtering and detection of malware threats, which enhance cyber security.

7.4 Parameters for developing the IT Disaster Recovery Plan

The Government of Punjab must develop an overall IT disaster recovery plan. It begins by compiling an inventory of hardware (e.g., servers, desktops, laptops, and wireless devices), software applications and data. The plan should include a strategy to ensure that all critical information is backed up.

Identify critical software applications and data and the hardware required to run them. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. Prioritize hardware and software restoration.

Document the IT disaster recovery plan as part of the business continuity plan. Test the plan periodically to make sure that it works.

7.4.1 Data Backup

Data backup and recovery should be an integral part of the business continuity plan and information technology disaster recovery plan. Developing a data backup strategy begins with identifying what data to backup, selecting, and implementing hardware and software backup procedures, scheduling and conducting backups and periodically validating that data has been accurately backed up.

7.4.1.1 Developing the Data Backup Plan

Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up along with other hard copy records and information. The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. Data on the server can then be backed up. Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

7.4.1.2 Options for Data Backup

Tapes, cartridges, and large capacity USB drives with integrated data backup software are effective means for backup of data. The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan. Backups should be stored with the same level of security as the original data.

Many vendors offer online data backup services including storage in the “cloud”. This is a cost-effective solution for businesses with an internet connection. Software installed on the client server or computer is automatically backed up.

Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not fatalistic to the services of the government.

7.5 Compliance Grid for Establishing a Business Continuity Plan

| Steps to be taken | Creator | Checker | Approver |
|---|----------|---------|----------|
| Step 1: PSDP Project Management Unit to develop IT recovery strategies based on system components mentioned | PSDP PMU | CDO | SDSC |
| Step 2: PSDP PMU to develop IT Disaster Recovery Plan based on parameter mentioned | PSDP PMU | CDO | SDSC |
| Step 2: PSDP Project Management Unit to ratify the plan through the Chief Data Officer and disseminate amongst the Departmental Data Cells of Department | PSDP PMU | CDO | SDSC |

