SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Data Sharing Policy

Document Classification: **Public**

Version 2.0

2024


بسم الله الرحمن الرحيم

Definitions

1. **Data:** A collection of facts in their raw or unstructured form, such as numbers, letters, static images, video, audio recordings, or emojis.
2. **Data Requester:** The public or private entity or the individual submitting a data-sharing request.
3. **Data Source Entity:** The government entity (as per its regulatory jurisdiction) responsible for setting the technical standards for a specific data field or a group of data fields, along with the standards for verifying their accuracy and retention.
4. **Authorized Entity:** The entity authorized to share data pursuant to an authorization granted by the Data Source Entity, in accordance with the procedures outlined in this Policy, and after taking the necessary steps to ensure the data is up-to-date.
5. **Data Sharing Entity:** The government entity that is requested to share data, whether it is the Data Source Entity or the Authorized Entity.
6. **Data Sharing Parties:** The Data Requester and the Data Sharing Entity.
7. **Data Sharing Agreement:** A standard agreement signed between two parties (when a government entity shares data with a private entity or individual) that (the standard agreement) defines the roles and responsibilities of the Data Sharing Parties in accordance with the provisions and controls specified in this Policy.

8. **Data Sharing Controls Template:** A standard template that includes the necessary controls for handling data and defining roles and responsibilities if the Data Sharing Parties are government entities.
9. **The Authority:** The Saudi Data & AI Authority (SDAIA).
10. **The Office:** The National Data Management Office (NDMO).
11. **Entity's Office:** The government entity's data management office.
12. **Government Service Bus:** A secure channel for data sharing among government entities to achieve integration and interoperability between entities and enable them to automate their services.
13. **Data Marketplace:** A platform designed to automate all data-sharing processes (subject to the provisions of this Policy) among government entities. The platform allows entities to request subscriptions to data-sharing services (APIs) published on the platform in an automated manner or to request new services. The Data Marketplace is one of the data platforms available at the National Data Bank (NDB).
14. **Metadata:** Detailed information that characterizes data and its utilization attributes, whether it be business, technical, or operational data.

First: Scope

1. The provisions of this Policy govern the sharing of government entity data with Data Requesters, irrespective of its form or nature. This includes, but is not limited to, paper records, emails, data stored on electronic media, audio or video recordings, maps, photographs, manuscripts, handwritten documents, or any other form of recorded data.
2. The provisions of this Policy do not apply to data-sharing processes when the Data Requester is a government entity and the request is for security purposes, to comply with judicial requirements, or in fulfillment of an international agreement to which the Kingdom is a party.
3. The provisions of this Policy do not apply when the Data Requester is a government entity and the data-sharing request is for the purpose of exercising regulatory functions or monitoring the performance of government entities in accordance with the Data Requester's systems or regulations, subject to compliance with the following:
   A. The data-sharing request shall be documented in a dedicated log by the data management office of the Data Sharing Entity.
   B. The Data Requester shall request only the minimum data required to fulfill the purpose for its collection and retention, while ensuring compliance with relevant laws and regulations or other relevant regulatory requirements.

C. Data sharing shall be conducted automatically through the Government Service Bus or other secure automated methods. In cases where automated sharing is not possible, and data sharing is to be conducted through non-automated means, the data sharing shall be performed through a secure and reliable method designated by the competent authorities.

D. Shared data shall be destroyed upon the fulfillment of its intended purpose, in compliance with relevant laws and regulations or other relevant regulatory requirements.

Second: The Main Principles for Data Sharing

First Principle: Data Sharing Culture

Each Data Source Entity shall share the data it produces in accordance with the provisions of this Policy, in order to enhance the utilization of such data and achieve integration among government entities.

Second Principle: The Single Source of Truth (SSOT)

Government entities shall collect data as a Single Source of Truth (in the context of exercising their statutory powers), with the possibility of sharing and reusing the collected data in a manner that does not conflict with any relevant regulations. This aims to reduce data duplication, inconsistencies, and disparate data sources, ensuring data integration, recency, and quality.

Third Principle: Legitimate Purpose

Data sharing shall be conducted for legitimate purposes that are grounded in a legal basis or justified operational need. Such data-sharing activities shall not compromise national interests, the operations of entities, individual privacy, or environmental safety. The shared data shall be used by the Data Requester solely for the purposes specified in the data-sharing request.

Fourth Principle: Authorized Access

All Data Sharing Parties shall be authorized to access, obtain, and utilize the shared data. Such access is granted through the identification and verification of authorized personnel (when necessary, such verification is contingent upon the data's nature, classification, and sensitivity level, as outlined in the Data Classification Policy).

Fifth Principle: Transparency

All necessary information pertaining to data-sharing requests shall be made available to all Data Sharing Parties. This includes a clear description of the requested data, its classification levels (as defined in the Data Classification Policy), collection purpose, storage methods, protection controls, and destruction mechanism.

Sixth Principle: Collective Accountability

All Data Sharing Parties shall be held collectively accountable for data-sharing decisions, consistent with the roles and responsibilities outlined in the Data

Sharing Agreement or applicable controls, as the case may be, to ensure data is processed in alignment with the specified purposes.

Seventh Principle: Data Security

All Data Sharing Parties shall implement appropriate security controls to protect data and ensure a secure and reliable data-sharing environment as per relevant regulatory requirements and directives issued by the National Cybersecurity Authority.

Eight Principle: Ethical Data Use

All Data Sharing Parties shall, in compliance with relevant regulatory requirements, adhere to ethical principles, to ensure responsibility, fairness, integrity, and trust in data use.

Third: The General Rules for Data Sharing

In accordance with the data sharing protocols established in Clause (Sixth), the following general rules shall govern data sharing among entities:

1. If the Data Requester is a government entity, data sharing is conducted automatically through the Government Service Bus.
2. If automated data sharing between government entities cannot be conducted through the approved methods outlined in Paragraph (1) of this Clause or if the Data Sharing Entity has valid justification, the Data Sharing Parties shall propose a secure and appropriate alternative method to the Office for approval.
3. If neither of the methods specified in Paragraphs (1) and (2) is possible, and

data sharing is to be conducted through non-automated means, the Data Sharing Parties shall conduct data sharing through a secure and reliable method designated by the competent authorities.

4. The Data Marketplace shall serve as the primary platform for inter-governmental data-sharing requests. In cases where data cannot be acquired through the Data Marketplace, government entities may submit requests to the Data Sharing Entity's Office for the publication of the requested data on the Government Service Bus, subject to the procedures determined by the Office.
5. If the Data Requester is a non-government entity, the data-sharing request shall be submitted to the relevant Data Sharing Entity's Office in accordance with the procedures determined by the Office.
6. Metadata shall be attached upon data sharing, with a clear specification of the classification levels of the requested data.
7. Data-sharing requests from government entities shall be subject to the Data Sharing Controls Template provided by the Office.
8. If the requested data is operational data and the Data Sharing Entity is neither the Data Source Entity nor the Authorized Entity, and the request does not include the consent of the Data Source Entity, the Data Sharing Entity shall notify the Data Requester within (5) business days of receipt of the request to obtain the consent of the Data Source Entity. The Data Source Entity shall respond to the request with approval or rejection, in whole or in part, provided

that any rejection shall be accompanied by a justification, within a period not exceeding (10) business days of the consent request.

9. If the Data Source Entity does not respond within the time period specified in Paragraph (8) of this Clause, this shall be deemed a rejection of the request. The Data Requester (as per the circumstances referred to in Paragraph (8) of this Clause) may then escalate the matter to the Office for consideration in accordance with the provisions of Paragraph (3) of Clause (Eighth) of this Policy.
10. The Data Sharing Entity may engage in data-sharing activities without the consent of the Data Source Entity if it has been authorized to do so under Clause (Fourth).
11. The Data Sharing Parties shall comply with the provisions governing competition when engaging in data-sharing activities and shall not enter into agreements that would prejudice relevant statutory provisions.
12. Subject to Paragraph (6) of Clause (Sixth), a data-sharing agreement shall be signed by the first officer or his/her duly authorized representative of the Data Sharing Entity if the requested data is classified as secret or top secret, and shall be signed by the director of the data management office of the Data Sharing Entity when the shared data is classified as restricted.
13. If the requested data is for analytical purposes, the data shall be requested from the National Data Bank. If this is not possible, it shall be acquired from

the Data Source Entity subject to the provisions of Paragraphs (1), (2), and (3) of this Clause.

Fourth: Data Sharing Authorization Request

1. The Data Sharing Entity may engage in data-sharing activities upon obtaining authorization from the Data Source Entity. Such authorization shall specify the following:
   A. The duration of the authorization and the process for renewal.
   B. The type of data and its classification level.
   C. The method of sharing, subject to the provisions of Clause (Third).
   D. The responsibilities and roles to ensure the security and protection of the data when shared with the Data Requester.
   E. The mechanism for resolving disputes arising from the authorization.
   F. Any other terms and conditions that the Data Source Entity (Authorizing Entity) deems necessary to include in the authorization.
2. The Data Source Entity (Authorizing Entity) may monitor the Authorized Entity's compliance with authorization requirements and request records of data-sharing requests and the shared data.
3. The Authorized Entity shall take the necessary steps to ensure the data is up-to-date before engaging in data-sharing activities.

Fifth: Mechanism for Determining Data Sharing Controls

All Data Sharing Parties shall determine the necessary controls to adequately manage and protect the data to be shared, as follows:

1. **Legal Basis:**

(Related Principles: First Principle: Data Sharing Culture. Second Principle: The Single Source of Truth (SSOT). Third Principle: Legitimate Purpose. Sixth Principle: Collective Accountability. Eighth Principle: Ethical Data Use).

A. The legal basis or the justifiable operational need for data sharing shall be established, including, for example, the entity's regulations or the relevant orders and decisions that qualify the entity to obtain the data.

B. Data confidentiality shall be maintained in accordance with its classification level, the privacy of Personal Data Subjects, and the protection of intellectual property rights.

2. Authorization:

(Related Principles: Fourth Principle: Authorized Access. Seventh Principle: Data Security).

A. Authorized personnel shall be appointed to request and receive data-sharing requests among the Data Sharing Parties in accordance with the Access and Usage controls stipulated in the Data Classification Policy. The authorized

personnel (with proper qualifications and training) shall be appointed to guarantee responsible handling of the shared data.

B. Authorization shall be granted based on the principle of need to know and the principle of least privilege when handling shared data, consistent with the provisions of the Data Classification Policy.

3. **Data Type:**

(Related Principles: First Principle: Data Sharing Culture. Second Principle: The Single Source of Truth (SSOT). Third Principle: Legitimate Purpose. Fifth Principle: Transparency).

A. Only the minimum amount of data necessary to achieve the specified purposes shall be requested.

B. Requests shall specify the data, its format, and the requirements to modify or change it, including data format, data accuracy, level of detail, data structure, and data type.

C. Agreed-upon mechanisms for updating previously shared data, if necessary, shall be specified between the Data Sharing Parties.

4. **Data Pre-processing:**

(Related Principles: Second Principle: The Single Source of Truth (SSOT). Seventh Principle: Data Security).

A. It shall be determined whether there is a need to preprocess the data before sharing. If so, the required processing methods shall be agreed upon, such as masking, anonymization, and aggregation (provided that the data processing does not impact its content).

B. The quality, validity, and integrity of the requested data shall be assessed to determine if it requires any improvement before sharing.

5. **Data Sharing Means:**

(Related Principles: Seventh Principle: Data Security).

A. Ensure the security and reliability of data-sharing channels if the means specified in Paragraph (1) of Clause (Third) cannot be utilized to mitigate potential risks, in accordance with regulatory requirements issued by the competent authorities.

B. The Data Sharing Parties shall agree in the data-sharing request on the data retention periods and data destruction mechanism upon fulfilling the data collection purpose, taking into account relevant regulatory requirements.

6. **Data Usage and Protection:**

(Related Principles: Third Principle: Legitimate Purpose. Fifth Principle: Transparency. Seventh Principle: Data Security. Eighth Principle: Ethical Data Use).

A. The specific data protection requirements applicable to the shared data shall be identified, and the specified controls shall be implemented to safeguard the data after sharing in accordance with its classification level.

B. Appropriate restrictions shall be imposed on the permitted use or processing of the data (if any), such as processing constraints, territorial or time limitations, or exclusive or commercial rights.

C. The rights of the Data Sharing Entity engaging in data-sharing activities, including the right to conduct audits and reviews, and its rights against any third party benefiting from the data, shall be determined.

D. Dispute resolution procedures shall be agreed upon.

E. It shall be ascertained whether a third party will derive benefit from the shared data, and the mechanism governing such beneficiary shall be agreed upon.

7. **Data Sharing Duration, Frequency, and Termination:**

(Related Principles: Third Principle: Legitimate Purpose. Seventh Principle: Data Security).

A. A specific duration for data sharing, including a deadline for data access or storage, shall be determined.

B. The frequency of sharing, the requirements for data review and modification, and the measures to be taken upon the termination of the agreement shall be specified, such as de-identification of Data Subjects, data access revocation, or destruction of data.

C. The parties authorized to terminate the data sharing before the agreed-upon end date, the legal grounds, and the permissible notice period, shall be specified.

8. **Liability Provisions:**

(Related Principles: Sixth Principle: Collective Accountability).

A. The parties shall agree on the determination of liability in the event of non-compliance with the terms of the agreement or any other obligations between the parties engaging in data-sharing activities.

B. The rules governing liability and compensation shall be defined in the event of the sharing of erroneous or inaccurate data, technical problems during the data transfer process, or accidental or unlawful loss of data that may cause other damages.

Sixth: Necessary Steps for Data Sharing

Data-sharing requests shall be processed in the following sequence:

1. Subject to the provisions of Paragraphs (4) and (5) of Clause (Third), the Data Requester shall submit a data-sharing request to the Data Sharing Entity's Office. This is applicable only if the Data Requester is also a government entity.
2. The Data Sharing Entity shall verify the classification level of the requested data. If the classification level is not specified, the Data Sharing Entity's Office shall classify the requested data in accordance with the Data Classification Policy.
3. The Data Sharing Entity's Office shall assess the request according to the following:
   A. There is a legitimate purpose for data sharing with a legal basis or justifiable operational need.
   B. The requested data conforms to the Data Minimization Principle to fulfill the sharing purpose.

C. The Data Source Entity has granted consent in cases where the data-sharing request was submitted to an entity other than the Data Source Entity or Authorized Entity.

4. If the request does not fulfill the requirements outlined in Paragraph (3) of this Clause, the Data Sharing Entity's Office may reject the request and provide a justification for the rejection. The Data Requester shall be afforded the opportunity to fulfill the requirements pursuant to Paragraph (2) of Clause (Seventh) Data Sharing Timeframe.
5. Upon fulfillment of all data-sharing requirements, appropriate controls shall be specified in alignment with clause (Fifth) to guarantee adherence to the data-sharing principles and achievement of their specific objectives.
6. If the Data Requester is a non-government entity, a Data Sharing Agreement shall be executed. If the Data Requester is a government entity, the controls specified in Paragraph (2) of Clause (Eighth) shall be satisfied.
7. Upon satisfaction of the conditions set forth in Paragraph (6) of this Clause, the requested data shall be shared with the Data Requester in accordance with the timeframes outlined in Clause (Seventh).
8. The provisions of Paragraphs (3) and (6) of this Clause shall not apply if the shared data is classified as public.

Seventh: Data Sharing Timeframe

1. The Data Sharing Entity's Office shall assess the request within a period not exceeding (10) business days of receipt of the request and provide the Data Requester with a written justification for its decision.
2. If the data-sharing request is rejected, the Data Requester shall have the right to fulfill the specified requirements and resubmit the request. Upon resubmission, the Data Sharing Entity's Office shall reassess the request and render a decision within five (5) business days of receipt.
3. Upon approval of the data-sharing request, the Data Sharing Entity's Office shall comply with the provisions of Paragraph (6) of Clause (Sixth), mandating the sharing of requested data with the Data Requester within (5) business days of approval, and subsequently within (10) business days of the completion of the procedures outlined in Paragraph (6) of Clause (Sixth).
4. If the processing of the request necessitates an extraordinary level of effort by the Data Sharing Entity, or if the nature of the request demands a timeframe exceeding that prescribed in this Policy, the Data Sharing Entity shall extend the processing timeframe and notify the Data Requester of the reason.
5. If the Data Sharing Entity fails to respond within the timeframe specified in Paragraph (1) of this Clause, the Data Requester may submit a written or electronic notice to the Data Sharing Entity's Office. The Data Sharing Entity's Office shall then follow up on the status of the request and notify the Data Requester of the reasons for the delay within a period not

exceeding (5) business days. If the Data Sharing Entity fails to respond within this period, the Data Requester may submit a notice to the Office for consideration as per Paragraph (3) of Clause (Eighth) of this Policy.

Eighth: Roles and Responsibilities

1. The Data Sharing Parties are committed to the security, protection, and use of data in accordance with the specified purposes, as stipulated in Principle (Seventh) of this Policy. The Data Sharing Entity's Office has the right to periodically review compliance under the mechanisms issued by the Office.
2. The Office shall prepare standard templates for:
   A. Data Sharing Request.
   B. Data Sharing Agreement.
   C. The controls referenced in Paragraph (7) of Clause (Third).
   D. Authorization Template.
3. In the event of a dispute between the Data Sharing Parties regarding the implementation of the provisions of the Policy, the parties may refer the matter to the Office for a legal opinion in accordance with the Office's determined procedure.
4. If the dispute is not resolved in accordance with Paragraph (3) of this Clause, the Office shall complete the necessary legal proceedings.
5. The Data Sharing Parties shall comply with all regulatory and other relevant requirements relating to the reporting of data leakage incidents.

6. If the request pertains to the sharing of personal data, the provisions of the Personal Data Protection Law, its Implementing Regulations, and the Disclosure Conditions outlined in the Law shall be considered.
7. Government entities shall retain records of data-sharing requests and related documentation for a period of five years following the termination of the data-sharing request.
8. The Data Sharing Entity's Office shall prepare and publish a policy for sharing its data in accordance with this Policy.
9. Government entities shall publish the approved contact information for their Office, such as the email address of the entity's data management office, to enable the submission of data-sharing requests.
10. Government entities shall implement the necessary technical, administrative, and organizational measures to ensure timely responses to data-sharing requests in compliance with the timeframe outlined in Clause (Seventh). For example, developing internal procedures manuals for responding to data-sharing requests, service-level agreements, and a matrix of internal authorities.
11. The Office shall monitor compliance with the provisions of this Policy. The Office may engage any external entity to monitor compliance in accordance with the procedures determined by the Office.

SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority