SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

National Data Governance Policies

Version 1 - 5/5/2020

Data Sharing Policy

3. Data Sharing Policy

3.1 Scope

The provisions of this Policy shall apply to all government entities vis-à-vis sharing the data produced by these entities – with other government entities, private sector entities, or individuals – regardless of its source, form, or nature. This shall include paper records, emails, information stored on electronic media, audio or video cassettes, maps, photographs, manuscripts or handwritten documents, or any other form of recorded information.

These Policies shall not apply to the sharing of the data owned by the private sector or by individual, nor to the case in which the data is requested by a government entity for security or judicial purposes.

3.2 Main Principles for Data Sharing

Principle 1: Data Sharing Culture

All government entities shall share the master data that they produce for the purpose of achieving integration among these entities. They shall adopt the "Single Source of Truth (SSOT)" principle to obtain the data from its proper sources and to avoid data duplication, inconsistency and multiple sources. If the data is requested from other than its main source, the entity required to share such data shall obtain the approval of the main entity, source of the data, prior to sharing such data with the requesting entity.

Principle 2: Legitimate Purpose

Data shall be shared for legitimate purposes based on a legal ground or a justified practical need that aims to deliver a public interest without inflicting any harm on national interests, entity activities, privacy of individuals or environmental safety, with the exception of data and entities exempted by Royal Orders.

Principle 3: Authorized Access

All the data sharing parties shall have the appropriate authority to access, obtain and use such data (a security clearance might be needed based on the nature and sensitivity of the data), as well as the knowledge, skills, and properly trained staff to handle the shared data.

Principle 4: Transparency

All the data sharing parties shall make available all information that is necessary for a successful data sharing process, including the required data, purpose of data collection, means of data transfer and storage, data security controls, and data disposal mechanism.

Principle 5: Collective Accountability

All the data sharing parties shall be held collectively accountable for the data sharing and processing decisions as per the defined purposes, and for ensuring the implementation of the security controls as defined in the Data Sharing agreement and as prescribed by relevant laws, regulations and policies.

Principle 6: Data Security

All the data sharing parties shall have apply the appropriate security controls to protect and share data in a secure and reliable environment as per the relevant laws and regulations, and in line with the National Cybersecurity Authority requirements.

Principle 7: Ethical Data Use

All the data sharing parties shall apply ethical practices throughout the Data Sharing process to ensure fairness, integrity, trust, and respect in data use, and shall not only comply with the information security policies or the relevant regulatory and legal requirements.

3.3 Data Sharing Process

The Data Sharing process has been designed to provide guidance to public entities on how to standardize the data sharing practices and ensure that all necessary controls and requirements are met. This Data Sharing Process shall be completed within a period not exceeding 3 months. Figure 3 below illustrates the steps required for the Data Sharing process.

1. The Requestor – whether a government or private entity or an individual – shall submit a data sharing request to the office of the entity requested to share the data, provided that said request is sent through the entity's office if the Requestor is a government entity.
2. The office of the entity requested to share the data shall forward the Data Sharing request to the relevant Business Data Executive who, in turn, shall assign one of the Business Data Stewards to address and evaluate that request.
3. The Business Data Steward shall check the classification level of requested data:

    a. If the classification level is not set, the office of the entity requested to share the data shall get the requested data classified as per the Data Classification Policy.

    b. If the classification level is assigned as "Public," the Business Data Steward may share the requested data without evaluating the request pursuant to the main principles of data sharing.

    c. If the classification level is assigned as "Restricted," "Secret," or 'Top Secret," the Business Data Steward shall evaluate the request pursuant to the main principles of data sharing.

4. The Business Data Steward at the office of the entity requested to share the data shall proceed with the data sharing process only if all Data Sharing principles are fully satisfied.
5. If one or more Data Sharing principles are not fully satisfied, the Business Data Steward at the office of the entity requested to share the data may not proceed with the Data Sharing process. In addition, the Business Data Steward shall return the request to the data requestor, along with the remarks, and shall give an additional chance to satisfy all the non-conforming Data Sharing principles.
6. When all Data Sharing Principles are satisfied, the Business Data Steward shall obtain the Business Data Executive's approval to proceed with the Data Sharing process.
7. The Business Data Steward at the office of the entity requested to share the data shall set the required controls to ensure compliance with the Data Sharing principles and meet the objectives set for each. Said Business Data Steward shall agree with the data requestor and all other parties of the Data Sharing process on implementing these controls.
8. After agreement on and strict compliance with the Data Sharing controls, the Business Data Steward shall provide clear details thereof in the Data Sharing Agreement; all parties involved in the sharing process shall sign the Data Sharing Agreement.
9. Once the Data Sharing Agreement is signed, the entity's office may share the requested data with the Requestor.

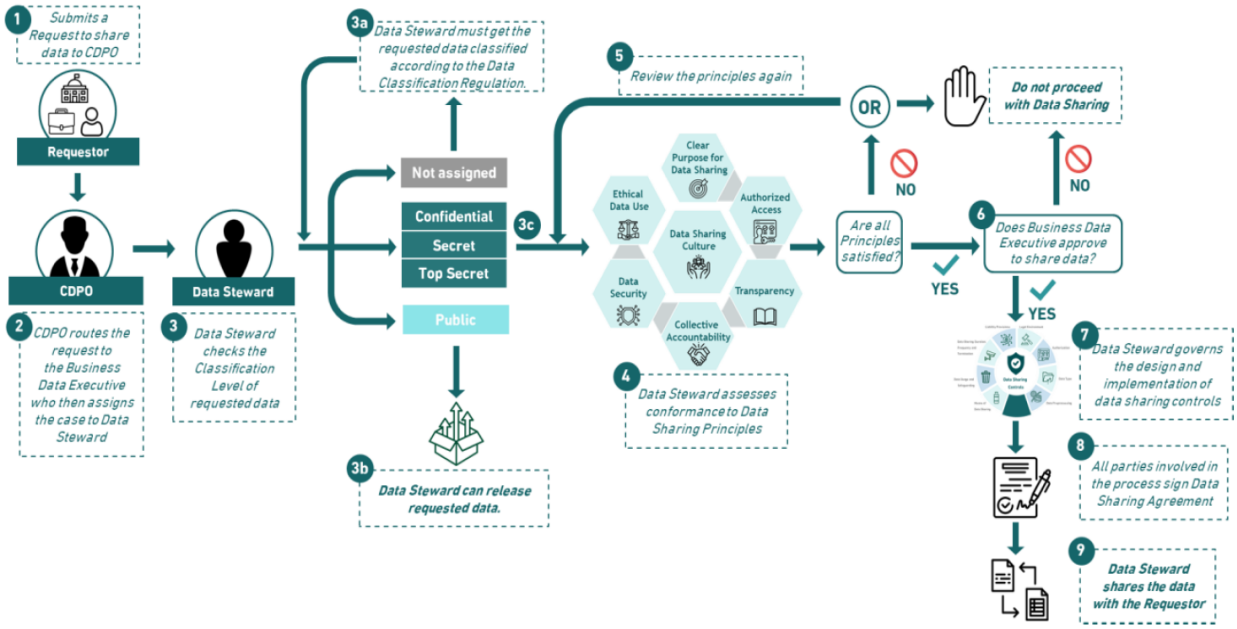

Figure 3: Data Sharing Process

3.4 Data Sharing Timeline

The government entity, required to share the data, shall evaluates the data sharing request within a period not exceeding 30 days from the date of receiving said request. It shall notify the Requestor of the data sharing decision, provided that the decision is written and reasoned (Steps 2-4 of the data sharing process described above).

In the event that the data sharing request is denied, the Requestor shall be entitled to complete the requirements to meet all the principles and request an appeal from the Business Data Steward to re-evaluate the request and issue the data sharing decision within a period not exceeding 14 days from the date of receiving the request (Step 5 of the data sharing process).

After obtaining the approval of the Business Data Executive to proceed with the sharing process (Step 6 of the Data Sharing process), the Business Data Steward shall develop and apply the appropriate Data Sharing controls and shall prepare a Data Sharing agreement within a period of time not

exceeding 60 days from the date on which the Business Data Executive granted his approval (Step 7 of the Data Sharing process).

After signing the Data Sharing agreement (Step 8 of the Data Sharing process), the Business Data Steward shall share the data with the Requestor within 7 days from the date of signing the agreement (Step 9 of the Data Sharing process).

3.5 Data Sharing Controls

All parties involved in the data sharing process shall agree to the controls necessary to appropriately manage and secure the shared data.

Legal Basis

(Relevant Principles: Principle 1: Data Sharing Culture; Principle 2: Legitimate Purpose; Principle 5: Collective Accountability; and Principle 7: Ethical Data Use)

- Clearly explain the lawful basis or actual need for data sharing (e.g. entity statute, Royal Order allowing the entity to share data, or signed agreements); and
- Comply with the data classification levels and preserve intellectual property rights and personal data privacy.

Authorization

(Relevant Principles: Principle 3: Authorized Access; Principle 6: Data Security)

- Identify the entities and individuals authorized to request and receive the data (check compliance with the Data Classification Policy, and data use and access controls).

Data Type

(Relevant Principles: Principle 1: Data Sharing Culture; Principle 2: Legitimate Purpose; Principle 4: Transparency)

- Ensure that the requested data is included in the master data produced by the entity to make sure that data is being requested from the right source;
- Specify the minimum volume of data required to satisfy the designated purposes; and
- Specify the type and format of the requested data and the requirements related to editing/changing such data (e.g. data format, data accuracy, level of detail, data structure, data type, whether raw or processed data).

Data Pre-processing

(Relevant Principles: Principle 6: Data Security)

- Decide if any data pre-processing is required before sharing and if so, agree on the required processing techniques to be used e.g. masking, anonymization, aggregation (as long as the data processing does not impact its content).
- Evaluate the quality, validity and integrity of the requested data and decide if it requires any improvement before sharing, in which case, the entity's office shall audit the data before sharing it.

Data Sharing Means

(Relevant Principles: Principle 6: Data Security)

- Comply with the data security controls issued by the National Cybersecurity Authority;
- Specify the physical and digital means of sharing data;
- Ensure the security and reliability of the data sharing means to minimize potential risks, as well as make use of the secure and approved sharing means between entities;
- Specify the Data Sharing mechanism and decide whether the Business Data Steward would directly transfer the data to the Requestor or the parties would utilize a professional service provider to carry out the Data Sharing process;
- Decide if the existing sharing mediums would be utilized (e.g. the Government Service Bus, National Information Center Network) or different mediums will have to be used (e.g. Wi-Fi, remote access, VPN, API, etc.); and
- Agree on the mechanism for destroying the physical mediums used in data sharing.

Data Usage and Protection

(Relevant Principles: Principle 2: Legitimate Purpose; Principle 4: Transparency; Principle 6: Data Security; Principle 7: Ethical Data Use)

- Specify the requirements for data protection upon its sharing and implement specific controls for data protection after sharing thereof;
- Set appropriate restrictions on the permitted use or processing of the data (if any), such as processing constraints, territorial or time limitations, or exclusive or commercial rights;
- Define the rights of all the data sharing parties to perform audits;
- Agree upon dispute resolution and arbitration procedures; and
- Determine whether there is a third party that would be using or handling the data after sharing it and agree on the mechanism for that accordingly.

Data Sharing Duration, Frequency and Termination

(Relevant Principles: Principle 2: Legitimate Purpose; Principle 6: Data Security)

- Specify the Data Sharing duration and the deadline for data access or storage;
- Set the frequency of sharing, review requirements, the process for amendments, and the measures to be taken upon the termination of the agreement (such as de-identification, data access revocation, or destruction of data).
- Identify the parties entitled to terminate the data sharing before the agreed-upon end date, legal grounds, and the permissible notice period.

Liability Provisions

(Relevant Principles: Principle 5: Collective Accountability)

- Determine liability in the event of non-compliance with the provisions of the Agreement, in addition to other obligations of the parties involved, such as agreement termination and corrective measures;
- Define the rules related to liability provisions upon sharing erroneous data, technical problems during the data transfer process, or accidental or unlawful loss of data that may cause other damages.

3.6 General Rules for Data Sharing

Following below is a set of general rules that entities are required to abide by in the data sharing process:

1. All entities shall prioritize the approved and secure data sharing mediums (e.g. the Government Service Bus, National Information Center Network) to transfer data.
2. The Business Data Steward at the office of the entity requested to share the data shall share data only after satisfying all the data sharing principles and determining all the appropriate controls for data sharing.
3. Each entity shall appoint or authorize the right person, as per the required qualifications and training, to handle the data properly, provided that he is authorized to request, receive, access, store, and destroy the shared data.
4. Personal data shall always be anonymized (de-identified) unless it is necessary for the sharing purpose along with setting the required controls to protect data privacy in line with the Personal Data Privacy Policy.
5. Metadata shall be provided upon sharing the data in cases so requiring.
6. Entities involved in Data Sharing shall be responsible for protecting the data and using it according to the defined purposes. The entity's office shall review such compliance on a periodical or ad-hoc basis subject to the controls set out in the Data Sharing agreement.
7. NDMO shall prepare a data sharing manual, to include templates for a data sharing request and for a standard data sharing agreement.
8. The regulatory authorities shall, upon coordination with NDMO, prepare the mechanisms, procedures and controls related to the settlement of disputes according to a specified timeframe.

9. In the event of a dispute between the parties involved in the Data Sharing process, if the entities are affiliated with the same Regulatory Authority, they shall be entitled to inform that Authority of the dispute and to demand a settlement thereof. If the dispute fails to be resolved, NDMO shall be notified of such failure. NDMO shall resolve the dispute if the two entities are not subject to the same Regulatory Authority.
10. Pertaining to any aspect of data sharing that is not covered in these Policies, the entity's office shall be entitled to set additional rules that do not conflict with the Data Sharing principles, provided that it presents adequate justifications for said rules and notify NDMO thereof.
11. The entities involved in Data Sharing shall adhere to appropriate balance between the need to share data and protect data confidentiality on the one hand and the potential risks to the individuals or the society.
12. Entitles shall maintain records of data sharing requests and the decisions related thereto.
13. Entities shall develop, approve, and publish their internal data sharing policy in accordance with these Policies.
14. Once shared data is received, entities shall not share same with any other party or entity without the consent of the entity producing such data.
15. The Entity shall be responsible for monitoring and implementing these Policies.