NDMO
مكتب إدارة البيانات الوطنية
National Data Management Office

National Data Governance Interim Regulations

Version 1

June 1st, 2020

Table of Content

1. Introduction

Government data represents a national asset that can enhance performance and productivity and facilitate public services delivery. This can be achieved by instituting effective data management practices, establishing the highest levels of data accountability and transparency, and leveraging data to extract insights and support strategic decision making. Nations around the world are harnessing the value of data as a vital economic resource for unlocking innovation, driving economic growth and transformation, and improving national competitiveness. Government entities in the Kingdom of Saudi Arabia collect and process vast amounts of data that can contribute to the national economic prosperity and leadership among global data-driven economies.

To drive full value realization from national data assets, data sharing is a foundational principle to establish synergies across government entities and avoid data duplication, inconsistencies, and multiple sources in absence of clarity regarding the single source of truth. This requires data classification against defined levels of confidentiality for balancing between the benefits and risks associated with data sharing among entities in the public, private, or third sector. Data classification is a pre-requisite for identifying and publishing open data, making publicly classified information available, and exchanging protected data that includes personal data. This increases the level of public scrutiny standards against the performance of public entities, enhances transparency, fosters integrity and removal of unnecessary secrecy on public entities' activities, supported by adequate procedures for the right to access public information otherwise known as Freedom of Information.

With the technological advancement and ease of access and sharing of data, personal data protection is becoming increasingly more critical which has instigated most countries around the world to release laws and regulations for collecting, processing, and sharing of personal data to protect individuals' right to privacy and to govern national data sovereignty.

The Kingdom of Saudi Arabia is paving towards a new era under the National Vision 2030, enhancing Government effectiveness and transparency, fostering economic diversification powered by digital and data, playing a larger role in the global economy, founded on public trust and international partnerships.

From this standpoint, the National Data Management Office (NDMO), as the national regulator of data in the Kingdom, has developed the framework for national data governance to set the policies and regulations required for data classification, data sharing, data privacy, Freedom of Information, open data and others in anticipation of necessary legislation. Considering the relationship and interdependencies of these policies and regulations as presented in Figure 1 below across the data lifecycle, NDMO has collated this Interim Regulations document to cover rules and obligations related to data classification, data sharing, data privacy, Freedom of Information, and open data.

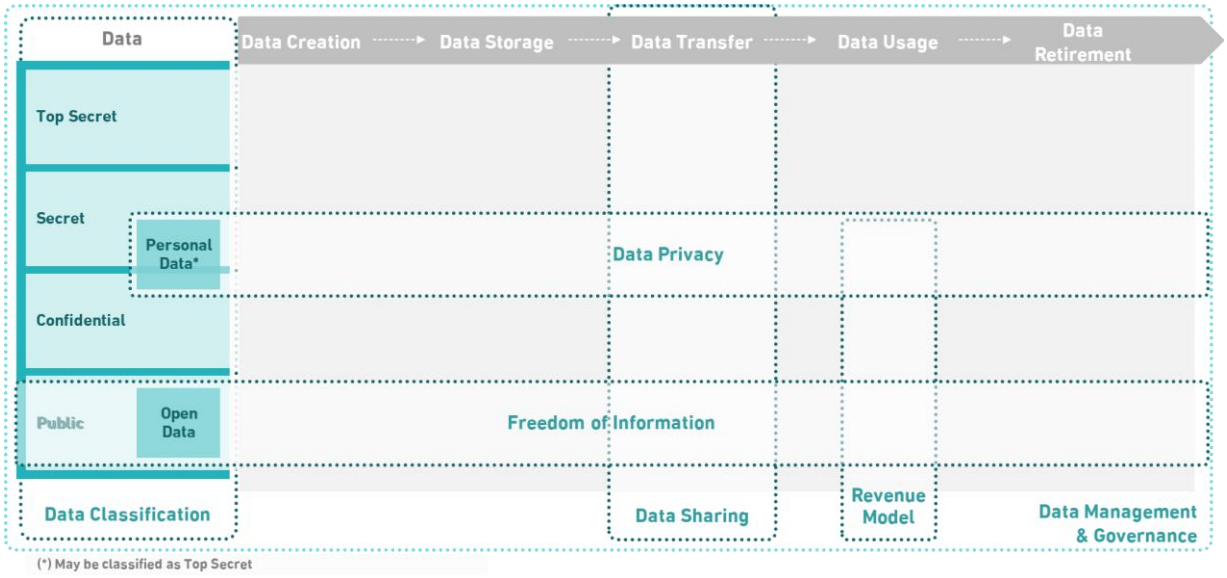

Figure1 – Relationship and Interdependencies of Data-specific Policies and Regulations

2. Definitions

For the purposes of this Interim Regulations, the following words and phrases, wherever mentioned herein, shall have meanings ascribed thereto, unless the context requires otherwise:

Data: A collection of facts in a raw or unorganized form such as numbers, characters, images, video, voice recordings, or symbols.

National Data: All data – regardless of form, source, or nature – that has been collected and processed within the jurisdiction of the Kingdom and under national sovereignty.

Personal Data: Is any element of data, regardless of source or form whatsoever, which independently or when combined with other available information could lead to the identification of a person including but not limited to: First Name and Last Name, Saudi National Identity ID Number, addresses, Phone Number, bank account number, credit card number, health data, images or videos of the person.

Data Access: Ability to view or make use of any data or resources in an information system of an entity.

Access Level: A category within a given security classification limiting data access to only authorized persons based on what is needed to complete their duties.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to data or resources in an information system.

Authorization: Access privileges to data or resources in an information system granted to a user, program, or process or the act of granting those privileges.

Data Availability: The state of making data accessible and usable when needed in a timely and reliable manner.

Data Confidentiality: The state of keeping data secret by preserving authorized restrictions on data access and disclosure.

Data Integrity: The state of ensuring data validity by guarding against improper information modification or destruction.

Restricted / Protected Data: Data classified as Confidential, Secret, or Top Secret.

Public Information: Raw data or processed data - unprotected - that is received, produced or held by public entities, regardless of the source, form or nature.

Open data: Datasets – that are machine-readable - made publicly available for free such that any individual, Business, or Public Entity can use or share it – considered a subset of Public Data.

Sensitive Data: Data, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of government programs, or the privacy to which individuals are entitled.

Requestor of Public Information / Applicant: the person applying for access to public information.

Data Subject: Any natural person to whom the personal data relates to, or his representative, or the person who has legal custody over him/her.

Personal Data Processing; Processing of personal data by any means, whether manual or automated processing, including collection, transfer, recording, storage, data-sharing, destruction, analysis, extraction of their patterns, conclusion and interconnection.

Data Controller: Any entity, or any natural or legal person, that collects Personal Data from a Data Subject and carries out processing of that Personal Data, directly or indirectly, through a processor, pursuant to a legal basis.

Data Processor: Any independent governmental or public entity, or any natural or legal person, which engages in the Processing of Personal Data, on behalf of a Data Controller pursuant to a legal basis.

Privacy Notice: Declaration directed towards data subjects that defines what personal data would be collected, the purpose behind processing it, how it would be used and which entities it would be shared with, the duration of its storage, and the means for disposing it.

Personal Data Destruction: Any action that leads to removal of personal data, rendering it impossible to view such Personal Data or retrieve it by any means, whether digital or physical.

Data Classification: Grouping data into levels based on the assessment of impact relating to unauthorized disclosure of the data or its content.

Data Classification Levels: One of the following: "Top Secret," "Secret," "Confidential," "Public."

Data Classification Marker: Marker or text assigned to classified data in specific ways to reflect the data classification level and its duration and to ensure adequate protection.

Disclosure of Personal Data: The intentional or unintentional access of Personal Data to any party, apart from Data Controller, Data Processor or Data Subject, allowing them to use or view same by any means and for any purpose.

Personal Data Breach: Disclosure, acquisition, or access to personal data in unauthorized form or in absence of a legal basis, whether intentionally or unintentionally.

Consent: A knowing, voluntary, clear, and specific, expression of consent, whether oral or written, from the Data Subject signifying agreement to the processing of their personal data.

Implied Consent: Consent of the Data Subject that is understood from their actions, certain events, or circumstances e.g. consent to the terms and conditions.

Third Party: A natural or legal person, public entity, agency or body other than the Data Subject, Data Controller, Data Processor, or authorized persons, involved in the processing of personal data.

Business Data Executive: The person who is ultimately responsible for specific data being collected and maintained by the Public Entity affiliated with, usually a member of senior management. A Public Entity may naturally have multiple Business Data Executives.

Business Data Steward: The person responsible for the business and technical deployment of the rules set forth by the Business Data Executive and for ensuring that the rules applied within systems are working, usually a member of Business, IT and/or Information Security departments.

Open data and Information Access Officer: The person responsible for the open data agenda and underlying activities, including planning, execution, and reporting.

Data User: Any person given the authority to access the data for reading, using, or updating it based on their responsibilities as authorized by the Business Data Executive.

Metadata: Information that describes data and its characteristics including business metadata, technical metadata, and operational metadata.

Machine-readable: Structured data in a specific format that can be automatically parsed and processed by a computer.

National Open data Portal: The central national portal dedicated for managing, storing, and publishing open datasets across the Kingdom.

Open data License: A legally binding instrument that grants permission to access, re-use, and redistribute open data with few or no restrictions.

Open Format: Any widely accepted, non-proprietary, platform-independent, machine-readable method for transmitting data, which permits automated processing of such data and facilitates analysis and search capabilities.

Data Requestor: The entity from the public, private, or third sectors or the individual submitting a request to share data.

Data Sharing Request: The dedicated form for requesting to share data that includes information about the Requestor, the data requested, and the purpose for which this data is requested.

Data Sharing Agreement: Data Sharing Agreement is a formal agreement signed between the Public Entity and another party to agree to share data according to certain terms and conditions that align with the data sharing principles.

Delivery Model for Data Sharing: The mechanism by which data will be shared. It includes the medium of transmitting the data, the parties involved in sharing, and the sharing model: direct sharing, sharing through a service provider, or through multiple parties.

Security Controls: Hardware, procedures, policies and physical and logical safeguards that are put into place to ensure the integrity and protection of data and the means of processing, accessing, and transferring it.

Public Entity: Any government or affiliated organization that manages, operates or maintains a public function or operates or maintains any elements of national infrastructure or provides a public service.

Regulatory Authority: Any independent governmental or public entity assuming regulatory duties and responsibilities for a specific sector in the Kingdom of Saudi Arabia under a legal instrument.

Entity's Office: The data management and privacy office within the public entity or the organizational unit responsible for data governance across the private and third sectors.

Chief Data and Privacy Officer (CDPO): The head of the entity's office. Therefore, an executive within the organization who has the authority and the influence to ensure that the data management and privacy program is followed by providing overall leadership for required initiatives and activities.

NDMO: National Data Management Office

3. Objectives

With reference to the Council of Ministers' resolution No. (292) dated 27/04/1441H., stating in Paragraph (1) of Article "Tenth" that NDMO is mandated to develop the policies, governance mechanisms, standards, and controls related to data and Artificial Intelligence and monitoring compliance against them post issuance, NDMO has analyzed global practices and standards to develop these Interim Regulations focused on national data governance that aim to:

1. Support the Kingdom's efforts towards achieving its vision and national strategies.
2. Establish a culture of data sharing and collaboration to enrich and develop data, information, and knowledge assets.
3. Managing the process of publishing, transferring, and using / reusing protected data and public information.
4. Achieve full integration across government entities.
5. Enabling government entities in developing their own policies, executing their plans, and forecasting to prepare for the future.
6. Protect personal data privacy and the confidentiality of sensitive data.
7. Protect individuals' right to data privacy when dealing with personal data and public information held by government entities.
8. Foster the open data concept and practices to enhance government transparency and promote research and innovation and drive economic growth.
9. Enhance transparency and establish governance rules through segregation of roles and responsibilities.
10. Protect national sovereignty specifically in relation to personal data.
11. Raise public scrutiny standards with regards to the performance of public entities.
12. Support efforts in fostering integrity and combating corruption by establishing access to public information as a human right.
13. Enabling entities to invest and innovate in services reliant on personal data to achieve social, economic, and competitiveness benefits and contribute to uplifting the Gross Domestic Product (GDP) of the Kingdom.
14. Foster trust in services reliant on data.
15. Raise the standard of services and electronic transactions, embracing complementarity.
16. Contribute to the development of the commercial and economic performance through transparency and fairness with regards to access to public information in order to enhance competitiveness while ensuring equal opportunity.
17. Evolve scientific research by encouraging researchers to benefit from public information and deliver on their social development and oversight role.

18. Provide equal opportunity for requestors of public information thereby reinforcing citizen equality and the collective awareness and participation in national matters.

Data Classification

Interim Regulations

4. Data Classification Interim Regulations

4.1. Scope

The Data Classification Interim Regulations applies to all data received, produced, or managed by public entities regardless of its source, form, or nature. This includes paper records, emails, information stored on computers, audio or video cassettes, microfiche, maps, photographs, handwritten notes or any other form of recorded information.

4.2. Key Principles

Principle 1: Open by Default

Data should be accessible (in development sectors) unless its nature or sensitivity requires a higher level of classification and protection; and top secret (in the political and security sectors) unless its nature or sensitivity requires a lower level of classification and protection.

Principle 2: Classification Based on Necessity

Where data must be classified, the level of classification, and the safeguards and controls associated with the classification level, should be based on the potential adverse impact as a result of unauthorized disclosure, subject to the nature and sensitivity of the data.

Principle 3: Timely Classification

Data should be classified upon creation or upon being received from another entity and the classification exercise should be timebound.

Principle 4: Highest Level of Protection

If information includes an integrated set of data with different classification levels, the highest classification level should be applied to the aggregated data.

Principle 5: Segregation of Duties

Duties of participants in the classification process should not overlap in terms of classifying data, approving a classification decision, granting authorization for access or usage of data, accessing data, protecting data, or disposal of data – in a way that does not lead to overlapping specialization or dissipation of liability.

Principle 6: Need to Know

Access to data should be provided only if there is legitimate requirement for usage of the data based on authorization and access controls and for the least number of people possible.

Principle 7: Least Privilege

Access to and use of data should be limited to the minimal access required to satisfy the needs of the assigned.

4.3. Data Classification Levels

Data Classification levels applicable to KSA public entities along with relevant impact levels, definitions and examples are outlined in the table below:

Classification	Impact Level	Definition	Examples
TOP SECRET "TS"	High	Data shall be classified as "Top Secret", if unauthorized access to or disclosure of such data or its content adversely and exceptionally affects in a way that is difficult to resolve: - National interest including violations of conventions and treaties, adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure and Government functions, **and/or** - KSA organizations functionality causing damage to the national interest, **and/or** - Individuals' health and safety at massive scale and privacy of Protected Individual personnel, **and/or** - Catastrophic damage to the environment or natural resources	- Military operations details and plans and any information related thereto - Official political information on the international relationships and conventions or treaties and all related discussions, studies and preparations - Information related to the activities, measures and structure of security and intelligence bodies. - Information on the encryption keys and mechanisms used for national infrastructure - Information on terrorism crimes and aggressive plans - Information on weapons and ammunitions or strategic military locations or any source of deterrent force - Information on movements of armed forces or internal security forces or VIPs movements - Information that affects the Kingdom's sovereignty

SECRET *"S"*	Medium	Data shall be classified as "Secret", if unauthorized access to or disclosure of such data or its content adversely affects: - Affects national interest such as damage to the reputation of the country, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure, Government functions, or the investigation of major cases such as terrorism funding **and/or** - Financial loss of KSA organizations that leads to bankruptcy or inability of the organizations to perform their duties or major loss of competitive abilities or combination thereof, **and/or** - Causes significant harm or injury impacting life of individuals - Causes long-term damage to the environment or natural resources	- Information on logistics storage or economic storages - Vital installations' information - Information on Memorandums of Understanding with the international companies to establish commercial or strategic economic interests in the Kingdom - Information related to bilateral agreements and diplomatic Memorandums of Understanding between the Kingdom and other countries

CONFIDENTIAL "C"	Low	Data shall be classified as "Confidential" data, if unauthorized access to or disclosure of such data or its content causes: - Contained negative affect on government entities' operations, KSA economy, **and/or** - Damage to any entity's assets and limited loss to its financial and competitive status, **and/or** - Negative effect on individuals' interests - Contained damage in the short-term to the environment or natural resources.	- Information that damages the reputation of a public figure - Detailed statements of individual transactions - Results of practical research and studies before publication thereof - Information related to products under manufacturing, which may damage fair competition - Sensitive administrative decisions and appointments information - Information on an individual's medical file - Personally Identifiable Information (PII) such as name, address, social security numbers, phone numbers, and account numbers, license numbers, biometric identifiers - Employees' salary information - Documents such as tactical level plans, marketing programs prior to public release, technology innovation plans - Vendor contracts and quotations - Requests for proposals - New product specification prior to public release - Design & implementation details of security systems (firewalls, access control, network diagrams, etc.) - Internal Entities Policies and Procedures - Internal Communications/Memos - Entities internal phone lists and email lists
PUBLIC **"P"**	None	Data shall be classified as "Public", if unauthorized access to or disclosure of such data or its content has no impact on: - National Interest, or - Organizations, or - Individuals, or - Environment	- National strategic trends. - National statistics on population, environment, businesses by industry, and others - Public development and economic studies. - Government acts and policies - Information on public services provided to citizens by Government - Organization contact persons - Advertisement for job postings - Public Announcements - Press releases - Publicly released financial results - Product presentations (Public) - Public relations information - Any information that is publicly available on organization websites - Advertisement

Table 1: Data Classification Levels

Data classified as "Confidential" can be further classified into one of the following sub-levels based on the impact of unauthorized access or disclosure as follows:

- **Confidential – Category (A):** if the impact is at the scale of a sector or across a general economic activity
- **Confidential – Category (B):** if the impact cuts across the activities of multiple entities or the interests of a group of individuals
- **Confidential – Category (C):** if the impact relates to the activity of a single entity or the interest of a specific individual

In establishing the appropriate classification levels, any and all potential risks should be considered from unauthorized access or disclosure of the data or its content and the table below illustrates many of the applicable factors (for more information on the impact assessment process, the "Data Classification Process" section provides further details).

Every entity – on its own – should conduct the impact assessment of unauthorized access or disclosure, and the list below is non-exhaustive.

Data Classification Levels			**Top Secret**	**Secret**	**Confidential**	**Public**
Impact Category	**Impact Sub-Category**	**Considerations**	**Level of Impact**			
			High	Medium	Low	None
National Interest	Reputation of the country	*Would the information be subject to international or national media interest? Would it give negative publicity?*	Reputation is adversely affected	Reputation is affected to some extent	Reputation is not affected	No impact on the National Interest
	Diplomatic Relationships	*Would the information drain or pose any risk to the relationship with friendly countries? Would it raise international tension? Could it lead to protests or sanctions from other countries?*	Diplomatic relationships and political affiliations are broken, and/or conventions and treaties terms are compromised	Diplomatic relationships are compromised and will be negatively affected in the long-term	No effect on the Diplomatic relationships or very minimal effect in the short-term	
	National Security / Public Order	*Would this information if released help with the identification or conduct of terrorist or serious crimes? Would it create an alarm to the public?*	Operational efficiency of the security or intelligence operations of military forces is significantly affected and compromised	Long-term effect on the ability and efficiency of the security and military forces to investigate or prosecute serious organized crimes causing internal operational instability	Impeding the detection of small crimes in the short-term with no to minimal effect in regional police operational stability	

	National Economy	*Would this information if disclosed cause losses to the overall KSA economy?*	Long-term effect on KSA economy with an unrecoverable decrease in the GDP, stock market rates, employment rate, purchasing power and/or other relevant indicators. All the country sectors are affected	Long-term effect on KSA economy with a recoverable decrease in the GDP, employment rate, stock market rates and/or purchasing power. One or more sector(s) are affected	Minimal or no effect on KSA economy with a quick recoverable decrease in the GDP, employment rate, stock market rates and/or purchasing power. Not more than one sector is affected	
	National Infrastructure	*Would the unrestricted access to such information cause any interruption of the critical assets of the country (i.e. Energy, Transport, Health…)? In case of a cyber-attack would the critical services of the country still available?*	Failure and long interruption of critical national infrastructure assets security and operations – Several sectors are affected, and normal life is interrupted	Failure and short interruption of critical national infrastructure assets security and operations – One or more sectors are affected	No effect or short-term effect on local/regional infrastructure assets security and operations	
	Government Functions	*Would the inadequate release of the information have the potential to limit the availability of the Government to carry out daily operations and business functions?*	All Government entities are impaired to conduct their functions and daily operations for a long period of time	One or more Government entities are not capable of delivering one or more of their functions for a short period of time	One or more Government entity non-core function(s) are compromised for a short period of time	
Organizations	Profits of the organization	*Would disclosure of this information lead to third parties' financial loss or bankruptcy? For example, consider possibility of fraud, illegal transfers of funds, illegal appropriation of assets*	High impact on the KSA organizations to the extent it causes damage to the national interest	Organization incurring heavy financial loss that could lead to bankruptcy	Limited damage to entity assets with limited financial loss	No impact on the Organizations
	Functions of the organization	*Would the release of this information cause any damage to private organizations of the country? Could it mean the loss of its leading role or of any of its assets? Would it lead to a significant number of employees being fired? Would it affect the competitiveness of the organization?*		Entity cannot perform any of its functions; severe loss of competitiveness	Entity cannot perform one of its key functions or the organization effectiveness has been reduced; Limited loss of competitiveness	

Individuals	Health/Safety of individuals	*Would the access to this information mean the release of names or locations etc.? (e.g. name and location of under-cover agents, people under protection orders)*	General or massive loss of life; Loss of life of an individual or group	Significant harm or life injury impacting life of an individual	Minor injury with no risk to the life or health of the individual	No impact on the Individuals
	Privacy	*Would compromise of this information violate the Data Privacy Regulation? Would it infringe any Intellectual Property Rights?*	Personal information of a VIP person has been disclosed affecting national interest	Personal information of a VIP person has been disclosed	Personal information of an individual has been disclosed	
Environment	Environmental Resources	*Would this information be used to develop any service/product that could potentially destroy environmental or natural resources of the country?*	Irrecuperable and catastrophic effect on the environment	Long-term damage to the environment	Short-term and limited damage to the environment	No impact on the Environment

Table 2: Data Classification Impact Assessment Categories and Levels

4.4. Data Classification Controls

Based on the data classification levels, appropriate data handling and protection controls shall be identified and implemented by entities to ensure secure handling, processing, sharing and disposal of data. If data is not classified at the time of creation or receipt as per the classification criteria, it shall be treated as "Confidential" until correctly classified.

Data Classification controls include but are not limited to (refer to the data protection controls and guidelines published by the National Cybersecurity Authority):

Protective Marking

- Protective marking – whether graphics or text – should be applied to paper and electronic documents (including emails) as per each classification level to provide the appropriate protection.

Access

- Access to data – logical and physical – shall be provided based on principles of "Least Privilege" and "Need-to-Know".
- Access must be revoked as soon as an individual's employment is terminated, reassigned, or suspended.

Usage

- Classified information shall be used as per the classification levels usage requirements. For example, "Top Secret" information shall only be used within specified locations whether physical (e.g. offices) or virtual (e.g. using cryptography or special applications).

Storage

- "Top Secret", "Secret" and "Confidential" data, or a mobile device that processes, stores or communicates "Top Secret", "Secret" and "Confidential" data shall not be left unattended.
- Unattended "Top Secret", "Secret" and "Confidential" data shall be protected while in storage either physically or electronically through National Cybersecurity Authority approved encryption mechanisms.

Data Sharing

- Entities shall decide on the physical and digital means of data sharing that ensure security, minimization of risk and compliance with Data Sharing regulations.
- Entities shall agree on the delivery model for Data Sharing, whether entities will utilize existing sharing mediums, e.g. Government Service Bus, National Information Center Network, or Secured Government Network, or will set up a new direct connection through wire, removable storage media, Wi-Fi, remote access / VPN, API, etc.

Retention

- A schedule defining the retention period of all data shall be maintained.
- The retention period shall be defined considering the applicable business, contractual, regulatory and legal requirements.
- The retention schedule shall be reviewed periodically – not less than annually – or when there are changes in applicable requirements.

Disposal

- All data shall be securely disposed of – in conformance with applicable Data Disposal Regulations – according to the retention schedule only after approval from the relevant Business Data Executive.
- "Top Secret", "Secret" electronically controlled data shall be disposed using electronic media disposal methods.
- All paper-based data shall be disposed of using cross shredder.
- A detailed log of all disposed of data shall be maintained.

Archival

- Data shall be archived in secure storage locations in the format recommended by the relevant Business Data Executive.
- Archived data shall be backed up.
- Archived "Top Secret" and "Secret" data shall be protected using National Cybersecurity Authority approved encryption mechanisms.
- A list of users authorized to access archived information shall be defined and documented.

Declassification

- Data must be declassified or downgraded when classification duration expires, or protection is no longer required at the original level.

- In case data has been wrongly classified, the data user must notify the Business Data Executive regarding the need to appropriately re-classify it.
- Data declassification triggers should be set when the initial classification is applied and should be captured in the data register. Triggers may include:
    - A set period after data creation or receipt (e.g. two years after creation)
    - A set period after the last action on an asset (e.g. six months after last use)
    - After a specific date has passed (e.g. to be reviewed on Jan 1st, 2021)
    - After circumstances that have a direct impact on the data change significantly (e.g. a change of strategic priorities or a change in government entities' employees).
- Declassification or creation of lower classification versions of data, outside of clear triggers, requires a sound understanding of both the sensitive data content and its context.

4.5. Data Classification Process

Step 1 – Identify all entity's data

The first step is to inventory all the data controlled by the entity.

Step 2 – Assign responsible of performing data classification

Upon completion of an inventory, the Entity must assign responsibility for performing the classification. It is usually the Business Data Executive, the person inside the organization who best understands the data, the one that should be responsible of making the initial classification. As there could be several Business Data Executives within the Entity, there could be more than one classifier.

Step 3 – Conduct impact assessment process

The Business Data Executive must follow an impact assessment process of the potential damages that could arise from:

- The disclosure of or the unauthorized access to such data,
- And/or unauthorized amendment or destruction of such data,
- And/or lack of access to such data in a timely manner.

The impact assessment process shall be initiated with the mindset of the 'Open by Default' principle (in the Development sector) unless its nature or sensitivity requires higher level of classification or protection; and Top Secret (in the Political and Security sectors) unless the nature or sensitivity requires lower level of classification.

Step 3.a – Identify the category impacted:

The first stage of the impact assessment process is to identify the impact that the compromise of the data could have on any of the following categories and subcategories:

- The national interest

- The organizations
- The individuals
- The environment

Step 3.b – Identify the level of the impact:

The second stage implies that the Business Data Executive must assign to each potential damage identified a level of impact. The impact level depends on:

- The impact duration and the difficulty to control the damage
- The time to recovery after the damage is caused
- The size of the impact (on a national level, regional, several entities, single entity, multiple individuals, etc.)

These parameters define the four levels of impact:

- **High Impact** – The compromise of such data could to cause extremely grave or critical damage and long-term nonrecoverable distress.
- **Medium Impact** – The compromise of such data could cause considerable or serious damage difficult to control or recover from in the short term.
- **Low Impact** – The compromise of such data could potentially lead to controlled or intermittent damages in the short-term and which are easy to control.
- **No Impact** – The compromise of such data is unlikely to cause any damage in the long or short term.

All risks identified through the impact assessment process should be specific and evidence-based, trying to limit the subjectivity of the person classifying the data .

Based on the identified impacts and their levels, the Business Data Executive shall assign a data classification level:

- High Impact -> data shall be classified as "Top Secret"
- Medium Impact -> data shall be classified as "Secret"
- Low Impact -> further assessments need to be considered (refer to Step 4 and 5)
- None -> data shall be classified as "Public"

A detailed description of the key considerations for each impact category and level is outlined in Table 2 'Data Classification Impact Assessment Categories and Levels.'

Consider step 4 and 5 whenever impact level identified is Low.

Go to step 6 if data has been classified as "Top Secret", "Secret" or "Public."

Step 4 – Consider compliance with existing regulations (only if impact level is Low)

When the impact level identified is Low and to maximize the data classified as "Public", additional assessments must be performed.

In this regard, the Business Data Executive must study whether the release of such data would conflict with the Kingdom's regulations including but not limited to the Anti-Cybercrime Law and the e-Commerce Law. If

the disclosure of the data would be against the laws and regulations, data should be classified as "Confidential", otherwise the Business Data Executive must continue to step 5.

Step 5 – Assess benefits of disclosure against potential negative impacts (only if the answer to step 4 is "NO")

After assigning a low level of impact and ensuring the disclosure of the data will not imply the breach of any existing law or regulation, entities must also assess the potential benefits of release of such data and consider whether those would outweigh the negative impacts. Potential benefits include the usage of the data for the development of new added-value services, an increased transparency of the government operations or greater involvement of the citizens with the government.

- If benefits > negative impacts -> data shall be classified as "Public"
- If benefits < negative impacts -> data shall be classified as "Confidential"

Step 6 – Review of classification level

The data classification reviewer – from the entity's data management office – must check all classified data to ensure the classification level assigned by the Business Data Executive is the most appropriate one. The review should take place within one month of the initial classification.

Step 7 – Apply controls

The last step of the data classification process is to ensure all data is protected as per its classification level by applying the relevant controls (refer to section 'Data Classification Controls').

The classification exercise is presumed to be concluded when 100% of the data owned by the entity is classified, its classification levels are verified, and the relevant controls are applied.

Post data classification, entities can share that data with other entities or make it available / publish it as open data in case the classification level is "Public."

The described process is illustrated in Figure 2.

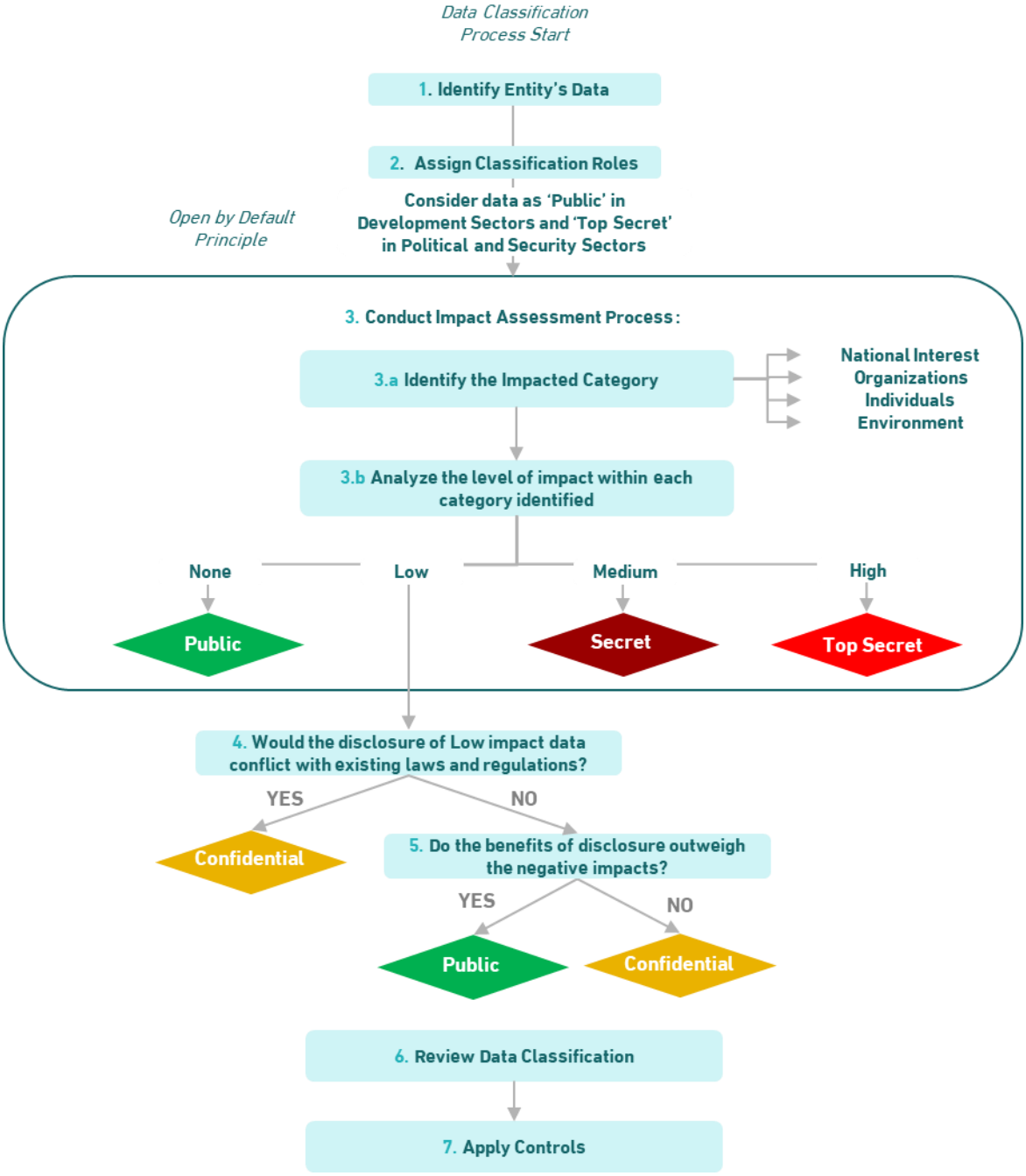

Figure 2 – Data Classification Process

4.6. Roles and Responsibilities Within the Entity

All Entities within the Kingdom shall designate individuals who will be responsible for carrying out the duties associated with each of the responsibilities within the data classification process as outlined below:

Business Data Executive - The person who is responsible for the data being collected and maintained by the entity, usually a member of senior management. The Business Data Executive shall address the following:

- **Data classification** – Classify all data collected by the entity and across entities that report to it.
- **Data compilation** - Ensure that data compiled from multiple sources is classified at the highest level of classification.
- **Data classification coordination** - Ensure that data shared between departments / entities is consistently classified and protected.
- **Data classification compliance (in coordination with Business Data Stewards)** – Ensure data is protected based on specific controls.

Data Classification Reviewer - The person who is responsible for reviewing and validating the data classification levels as defined by the Business Data Executive, usually a member of senior management.

Business Data Steward - The Business Data Stewards are usually existing members of the Business and/or IT and/or Information Security departments. They are responsible for ensuring the data is secured by applying the required controls as per the Data Classification Controls section. Data Steward responsibilities include but are not limited to:

- **Access control** - Ensure that proper access controls are implemented, monitored and audited in accordance with the Data Classification levels assigned by the Business Data Executive.
- **Audit reports** - Submit an annual report to the Business Data Executives that addresses availability, integrity and confidentiality of classified data.
- **Data backups** - Perform regular backups of data.
- Data validation - Periodically validate data integrity.
- **Data restoration** - Restore data from backup media.
- **Monitor activity** - Monitor and record data activity, including information on who accessed what data.
- **Data Classification compliance (in coordination with Business Data Executives)** - Ensure that entity's data is classified and secured following the process described in these Interim Regulations and in accordance with the defined controls.

Data User - The employee who manages, accesses, uses, or updates the data to complete a task authorized by the Business Data Executive. Data users benefit from the data in line with set purposes and in compliance with these Interim Regulations and all policies related to data usage across the Kingdom.

The head of the entity assigns the above roles to the qualified people within the entity.

Personal Data Protection

Interim Regulations

5. Personal Data Protection Interim Regulations

5.1. Scope

The Personal Data Protection Interim Regulations apply to all entities in the Kingdom that process personal data in whole or part, as well as all entities outside the Kingdom that process personal data related to individuals residing in the Kingdom using any means, including online personal data processing.

This Interim Regulations shall not be applicable to the direct collection of personal data – without informing the Data Subject - or its processing other than the purpose for which personal data has been collected or disclosed – without Data Subject's consent – or transferred outside the Kingdom, for the following cases:

1. If the Data controller is a government entity and the collection or processing of personal data is required for security purposes, to enforce another law, to fulfill judicial requirements, or to fulfill an obligation under an agreement to which the Kingdom is a party.
2. If the collection or processing of personal data is necessary to protect public health or safety or to protect the vital interests of individuals.

5.2. Key Principles

Principle 1: Accountability

Data Controller's privacy policies and procedures shall be identified, documented and approved by the head of entity (or his designee) and circulated to all concerned parties.

Principle 2: Transparency

A notice of Data Controller's privacy policies and procedures – Privacy Notice – shall be drawn up indicating the purposes for which personal data will be collected in a clear, easy to understand language.

Principle 3: Choice and Consent

The purpose for collection of any personally identifying data shall be shall be made clear to Data Subject and their (implicit / explicit) approval shall be obtained regarding collection, use and/or disclosure of personal data before collection.

Principle 4: Limiting Data Collection

Collection of any personal data shall be limited to minimum data that enables fulfillment of purposes provided for in Privacy Notice.

Principle 5: Use, Retention and Destruction

Personal data usage shall be restricted to purposes provided for in Privacy Notice, which the Data Subject has implicitly or explicitly approved. Moreover, Data shall be retained as long as necessary to achieve their intended purposes or as required by laws and regulations. Furthermore, data shall be destroyed it in a safe manner that prevents leakage, loss, theft, misuse or unauthorized access.

Principle 6: Access to Data

Entities shall provide a means by which any Data Subject can review, update and correct their personal data.

Principle 7: Data Disclosure Limitation

Disclosure of personal data to third parties shall be restricted to the purposes provided for in Privacy Notice, which was approved by Data Subject.

Principle 8: Data Security

Personal data shall be protected from leakage, damage, loss, theft, misuse, modification, or unauthorized access – according to the controls issued by the National Cybersecurity Authority and the relevant authorities.

Principle 9: Data Quality

Personal data shall be maintained after verification of its accuracy, completeness and timeliness, and such data shall be directly relevant to purposes provided for in Privacy Notice.

Principle 10: Monitoring and Compliance

Compliance with Data Controller's privacy policies and procedures shall be monitored, and any privacy-related inquires, complaints, and disputes shall be addressed.

5.3. Data Subject Rights

First: The right to be informed of the Legal Basis and the purpose concerning the collection and processing of their personal information. Personal Data may not be collected or processed without Data Subject's express consent and all processing must be consistent with the agreed upon Legal Basis.

Second: The right to withdraw his consent – at any time – unless statutory or judicial requirements require otherwise.

Third: The right to access his personal data within the possession of the Data Controller, including access to, request to correct, complete or update personal data, and request to destroy unnecessary data, and get a copy of such data in a clear format.

5.4. Data Controller Obligations

1. The Data Controller shall be accountable for development and enforcement of policies and procedures in respect of personal data protection. The head of entity (or his designee) shall be accountable for approval of such policies and procedures.

2. The Data Controller shall establish an organization unit (linked to CDO Offices across government agencies that have been established under the Royal Decree No. 59766 dated 20/11/1439 AH), or independent (for private sector institutions). This unit shall be entrusted with development, documentation, and monitoring implementation of the policies and procedures adopted by Controller's senior management/governance committee. The functions and responsibilities of the unit shall include development of appropriate standards to determine data sensitivity levels and the security measures required for each level.

3. The Data Controller shall assess the potential risks and impacts of specific activities. Evaluation results shall be presented to the head of the entity (or his designee) to determine and approve the acceptable risks.
4. The Data Controller shall review and update Service Level Contracts and Agreements in accordance with privacy policies and procedures adopted by Controller's senior management/governance committee.
5. The Data Controller shall prepare and document procedures necessary to manage and address privacy violations and to set the functions and responsibilities for the concerned work team, as well as the cases in which the Regulatory Authority and NDMO are notified according to reporting lines - based on measuring impact severity.
6. The Data Controller shall launch awareness programs to promote and raise awareness of privacy culture in accordance with privacy policies and procedures adopted by the Controller's senior management/governance committee.
7. The Data Subject shall – at the time of data collection – be duly notified of the purpose and legal justification/actual requirement, means and methods used to collect, process and share personal data as well as security measures to ensure that data privacy is maintained in accordance with laws and regulations.
8. The Data Subject shall be notified of other sources that are used in case all data are indirectly collected (from other parties).
9. The Data Subject shall be notified of available options in respect of personal data processing, and the available mechanism to exercise these options, for example (Preferences, Opt-in and Opt-out).
10. The Data Subject's approval shall be obtained for personal data collection, processing and sharing after determining the approval type (explicit or implicit) based on the data nature and collection methods.
11. Purpose of data collection shall be compliant with the laws and be directly related with the Data Controller's activity.
12. Data content shall be limited to the minimum data required for achieving the purpose of collection.
13. Data collection shall be limited to the pre-prepared content (as described in Rule no. 12) and shall be in a fair manner (Direct, clear, secured and not fraudulent or misleading).
14. Data shall be used only for the purpose for which it is collected.
15. The Data Controller shall prepare and document data retention procedures and policy in accordance with the relevant purposes, laws and regulations.
16. The Data Controller shall store and process the personal data within the Kingdom's territory in order to ensure preservation of the digital national sovereignty over such data. These personal data may only be processed

outside the Kingdom after the Controller obtains a written approval from the Regulatory Authority and the Regulatory Authority shall coordinate with NDMO.

17. The Data Controller shall prepare and document data erasure procedures and policies in order to destroy the data in a secure manner, that prevents data loss, misuse or unauthorized access – including operational and archived data and backups – according to controls issued by the National Cybersecurity Authority.
18. The Data Controller shall include data retention and destruction policy provisions in any agreements to be concluded with other Data Processors.
19. The Data Controller shall determine the means through which the Data Subject can access his personal data for the purpose of data review and updating.
20. The Data Controller shall verify Data Subject's identity before granting him access to his personal data according to the controls approved by the National Cybersecurity Authority and the relevant authorities.
21. Personal data shall not be shared with any other entities except for the purposes specified subject to the Data Subject's approval and according to the laws and regulations; provided that these other entities are provided with the relevant privacy procedures and policies and such procedures and policies are included in the contracts and agreements concluded therewith.
22. The Data Subject shall be notified, and his approval shall be obtained if his data are to be shared with other entities to be used in other purposes.
23. The Data Controller shall obtain NDMO's approval – having coordinated with the Regulatory Authority – prior to sharing the personal data with other entities outside the Kingdom.
24. The Data Controller shall develop and document the steps necessary for ensuring that the personal data are accurate, integral, updated and used for the purpose for which they are collected.
25. The administrative guidelines and technical measures adopted by the Controller for information security shall be followed in order to ensure personal data protection, including but not limited to:
    - Grant data access privileges in accordance with employees' duties and responsibilities.
    - Apply the administrative procedures and technical measures that document data processing stages and allow identifying the user responsible for each stage (processing records).
    - Employees who are initiating data processing operations sign a nondisclosure and confidentiality undertaking to only disclose such data in accordance with the policies, procedures, laws and regulations.
    - For data processing, the honest and responsible employees shall be assigned according to data nature and sensitivity and access policy approved by the Controller.

- Use the appropriate security measures (For example: Encryption, and separate the environments relating to development) in order to protect personal data in accordance with data nature and sensitivity and means used to transfer and store data according to controls approved by the National Cybersecurity Authority and the relevant authorities.

26. The Data Controller should periodically monitor compliance with privacy procedures and policies and present the same to the head of the entity (or his designee). The corrective procedures to be taken should be determined in case of non-compliance and the Regulatory Authority and NDMO should be notified according to the reporting lines.

5.5. General Dispositions

First: Regulatory Authorities shall ensure that the provisions of this document are line with their organizational documents and circulate the same to all its affiliates or relevant agencies in order to achieve integration and ensure achievement of targeted objectives.

Second: Regulatory Authorities shall monitor compliance with this Interim Regulation.

Third: Data Controllers shall comply with this Interim Regulation and document this compliance according to mechanisms and procedures established by Regulatory Authorities.

Fourth: Data Controllers shall notify the Regulatory Authorities immediately, no later than 72 hours in the event of any data breach or leakage impacting personal data in accordance with the mechanisms and procedures determined by the Regulatory Authorities.

Fifth: Data Controllers shall periodically, when contracting with Data Processors, verify that those data processors comply with this Interim Regulation according to mechanisms and procedures established by Regulatory Authorities, including any subsequent contracts concluded by the data processors.

Sixth: NDMO shall exercise the roles and functions of Regulatory Authorities over Data Controllers that are not subject to Regulatory Authorities.

Seventh: Regulatory Authorities shall develop additional rules to address specific types of personal data according to data nature and sensitivity after coordination with NDMO.

Eighth: Regulatory Authorities – in coordination with NDMO – share develop the mechanisms, procedures, and controls related to resolving complaints within a specific timeframe.

Ninth: NDMO shall set the necessary criteria to help Data Controllers assess whether the appointment of a Data Protection Officer is mandatory or optional.

Data Sharing

Interim Regulations

6. Data Sharing Interim Regulations

6.1. Scope

The Data Sharing Interim Regulations applies to all government data to share the data that is produced by these entities – with other public entities, private sector, or individuals – regardless of its source, form, or nature. This includes paper records, emails, information stored on computers, audio or video cassettes, microfiche, maps, photographs, handwritten notes or any other form of recorded information.

These Interim Regulations do not apply to sharing of private sector or individuals' data or data requests made by a governmental agency for security or judicial purpose.

6.2. Key Principles

Principle 1: Data Sharing Culture

All Government entities act as a Single Source of Truth (SSOT) for the data they produce. Hence, entities shall request data from SSOTs directly to avoid its duplication, inaccuracy, and storage in multiple sources rather than recreating it themselves or requesting from third parties. If the request to share data is submitted to the entity that acts as a data custodian of Government data and is not its SSOT, then a permission to share from SSOT is mandatory.

Principle 2: Clear Purpose for Data Sharing

The Data Requestor should clearly state the reason or legal basis behind the request for sharing data - except for data and entities exempted by a Royal Decree. Data should only be shared when it delivers a public benefit and would not inflict harm against national interests, organizations, individuals, or the environment.

Principle 3: Authorized Access

All parties involved in Data Sharing should have the appropriate authority (security clearance might be needed based on the nature and sensitivity of the data), knowledge, and skills along with properly trained staff to handle shared data.

Principle 4: Transparency

All parties involved in Data Sharing should make available all information that is necessary for the successful delivery of the Data Sharing purpose including required data, purpose behind data sharing request, data transfer and storage mechanism, data security controls, and data disposal mechanism.

Principle 5: Collective Accountability

All parties involved in Data Sharing should be held accountable for Data Sharing decisions, for processing it according to the defined purposes, and for taking the necessary actions to ensure data quality and implementation of security controls as defined in the Data Sharing agreement and as prescribed by relevant national laws and regulations.

Principle 6: Data Security

All parties involved in Data Sharing should have an adequate set of security controls to protect and safeguard data and enable a secure environment for Data Sharing in line with relevant national laws and regulations, and in line with the National Cybersecurity Authority requirements.

Principle 7: Ethical Data Use

All parties involved in Data Sharing should apply ethical practices throughout the Data Sharing process to ensure fairness, integrity, trust, and respect, and go beyond meeting data protection and security standards or other regulatory requirements.

6.3. Data Sharing Process

The Data Sharing process has been designed to provide guidance to public entities on the standardization of sharing practices to ensure all necessary controls and requirements are met . The Data Sharing Process, graphically depicted in Figure 3 below, should be completed within three (3) month of the initial request, has the following steps:

1. The Data Sharing process starts with a Data Sharing request from the data requestor – public sector, private sector, or individual - submitted to the receiving entity's data management office.
2. The receiving entity's office forwards the Data Sharing request to the relevant Business Data Executive who then assigns one of the reporting Business Data Stewards to manage and evaluate the Data Sharing request.
3. The Business Data Steward first checks the classification level of requested data:
    a. If the classification level is not assigned, then the entity's office – that has received the data sharing request - must get the requested data classified according to the Data Classification Interim Regulations
    b. When the classification level is assigned as 'Public', the Business Data Steward can release requested data without assessing conformance to the Data Sharing principles
    c. If the classification level is assigned as 'Confidential', 'Secret' or 'Top Secret', then the Business Data Steward must assess conformance to the Data Sharing principles.
4. The Business Data Steward shall continue the data sharing process only if all Data Sharing principles are satisfied.
5. If one or more Data Sharing principles are not fully satisfied, the Business Data Steward cannot proceed with the Data Sharing. Nevertheless, the Business Data Steward should return to the data requestor with the outcome of the evaluation reflecting the proper justification and give an additional chance to satisfy all principles.
6. When all Data Sharing Principles are satisfied, the Business Data Steward must get the Business Data Executive's approval to proceed with the process.

7. The Business Data Steward defines and sets the required controls that satisfy Data Sharing principles and meet the objectives set for each. The Business Data Steward must agree with the data requestor and all other parties that might be involved in the Data Sharing process on implementing these controls.

8. After agreeing on the Data Sharing controls and their implementation, the Business Data Steward should detail them in the Data Sharing Agreement that all parties involved in the sharing process should sign.

9. Finally, once the Data Sharing Agreement is signed, the entity's office shares the data with the Data Requestor.

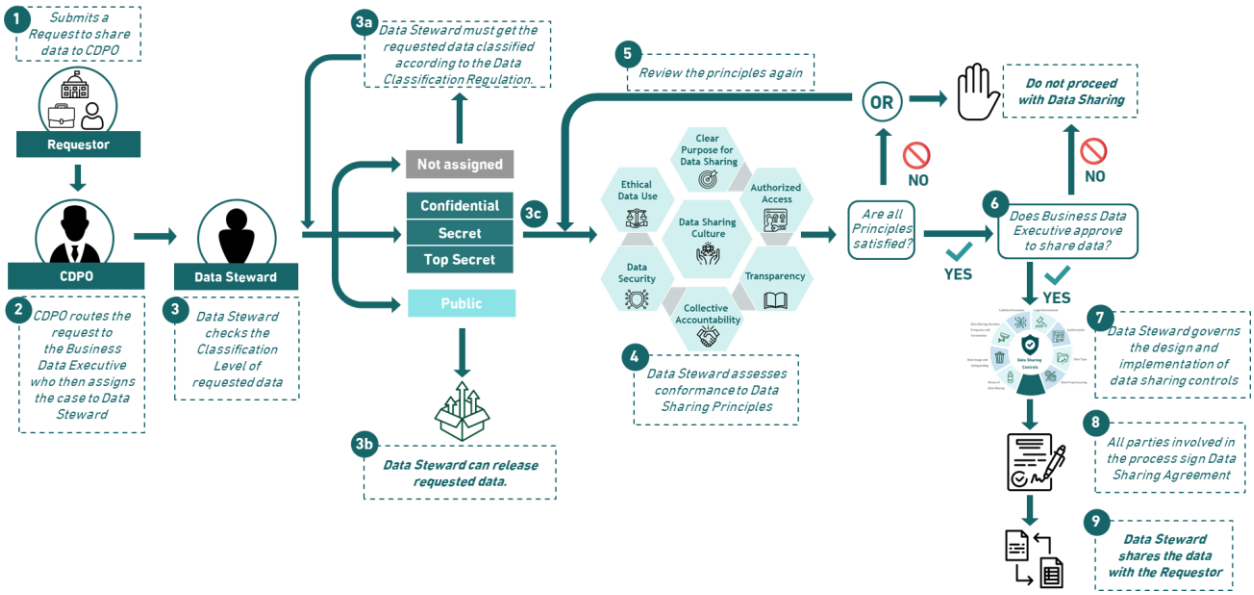

Figure 3 – Data Sharing Process

6.4. Data Sharing Timeline

After receiving a Data Sharing request, the public entity has 30 days to evaluate it, assess if all Data Sharing Principles are satisfied, formulate a written decision whether to share the data, and communicate it to the data requestor along with the proper justification (steps 2-4 of the Data Sharing process presented above).

If the decision is not to share the data, the data requestor is entitled to improve on non-compliant principles and appeal the Business Data Steward to re-evaluate the updated Data Sharing request. In that case, the Business Data Steward has 14 days to re-assess the request and provide a final decision (step 5 of the Data Sharing process).

After obtaining an approval from the Business Data Executive to proceed with Data Sharing (step 6 of the Data Sharing process), the Business Data Steward shall govern the design and implementation of Data Sharing controls which should not take longer than 60 days from the time the Business Data Executive provided the approval (step 7 of the Data Sharing process).

After signing the Data Sharing Agreement (step 8 of the Data Sharing process), the Data Steward has 7 days from the data of signing the Agreement to share the data with the data requestor (step 9 of the Data Sharing process).

6.5. Data Sharing Controls

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

Legal Basis:

(Supported by Principle 1 – Data Sharing Culture, Principle 2 – Clear Purpose for Data Sharing, Principle 5 – Collective Accountability, Principle 7 – Ethical Data Use)

- Clearly explain the lawful basis or need for sharing the data (e.g. entity mandate, royal decree allowing entity to share data, signed agreements).
- State how Intellectual Property Rights, Data Classification, and Data Privacy regulations would be preserved.

Authorization

(Supported by Principle 3 – Authorized Access, Principle 6 – Data Security)

- Define who are the individuals authorized to request and share data (check compliance with Data Classification Interim Regulations for usage and access controls).

Data Type

(Supported by Principle 1 – Data Sharing Culture, Principle 2 – Clear Purpose for Data Sharing, Principle 4 – Transparency)

- Check that the Sharing Entity is the SSOT for requested data (has the master data) to ensure data is being requested from the right source.
- Specify the minimum volume of data needed to satisfy the purpose of the sharing request.
- Specify the type and format of the shared data and the requirements related to editing/changing them (e.g. data format, level of detail, structured or unstructured, raw data, processed data).

Data Preprocessing

(Supported by Principle 6 – Data Security)

- Decide if any data preprocessing is required before sharing and if so, then agree and detail out the processing techniques used e.g. masking, anonymization, aggregation (as long as this does not impact the content of the data).

- Evaluate the quality of requested data and decide if it requires an improvement before sharing. If needed, the entity's office should prepare and cleanse the data before sharing it.

Means of Data Sharing

(Supported by Principle 6 – Data Security)

- Conform to the data security controls defined by the National Cybersecurity Agency.
- Specify the physical and digital means of sharing data.
- Ensure that the means of sharing are secure, and risks are minimized. If applicable, leverage existing secure and approved sharing mediums between entities.
- Specify the delivery model for Data Sharing. Decide if the data would be directly transferred to the Requestor or the parties would utilize a professional service provider to carry out the Data Sharing.
- Define if existing sharing mediums would be utilized (e.g. Government Service Bus, National Information Center Network) or new ones will have to be implemented (e.g. Wi-Fi, remote access / VPN, API).
- Agree on the mechanism for destroying the physical media used to share data.

Data Usage and Safeguarding

(Supported by Principle 2 – Clear Purpose for Data Sharing, Principle 4 – Transparency, Principle 6 – Data Security, Principle 7 – Ethical Data Use)

- Specify the requirements to safeguard data once shared. Specific controls should be applied in order to properly protect and secure data after sharing is completed.
- Set appropriate restrictions to the permitted use/manipulation of the data (if any), such as processing constraints, territorial or time limitations, exclusivity or commercialization rights.
- Define the rights of both parties to perform audits on the respect of the mutual obligations.
- Agree upon dispute resolution process and arbitration process.
- 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

(Supported by Principle 2 – Clear Purpose for Data Sharing, Principle 6 – Data Security)

- Specify the Data Sharing duration and deadline for accessing/storing the data.
- Set the frequency of sharing, any review requirements, the process for amendments, and measures to be taken after the agreement ends (such as de-identification, access revoke or destruction).
- State who has the rights to terminate the sharing before the agreed end date and on which legal grounds and what notice period.

Liability Provisions

(Supported by Principle 5 – Collective Accountability)

- Develop the roles and responsibilities for the parties involved in the Data Sharing as part of the Data Sharing Agreement as well as allocation of liability in cases of breaching the Agreement, in addition to other obligations related to corrective actions and terminating the Agreement.
- Agree on allocation of liability for contract breaches and other liabilities between the parties as part of the Data Sharing Agreement, as well as indemnification and other remedies when breaches occur.
- Define the rules on liability provisions for supply of erroneous data, disruptions in the data transmission, or unlawful/accidental loss of data that may potentially cause damages.

6.6. General Rules and Obligations

Below are a set of rules and obligations that entities involved in the sharing process are requested to follow:

1. All Public Entities should prioritize existing approved and secure sharing mediums (e.g. Government Service Bus, National Information Center Network) to transfer data.
2. The Business Data Steward can share data only when all principles are satisfied, and all controls and requirements assigned to the data are met and satisfied.
3. All entities are responsible for assigning the right person(s) who have the required qualifications and are sufficiently trained to handle the data properly and authorized to request, receive, access, store, and destroy shared data.
4. Data should always be anonymized (de-identified) from personal identifiers, unless it is necessary for the usefulness of the shared data while setting the required controls to protect data privacy in line with Data Privacy Interim Regulations.
5. The metadata of the shared data should be specified and provided when needed.
6. Entities involved in Data Sharing are responsible for protecting the data and using it according to defined purposes. The entity office can audit compliance periodically or ad-hoc basis subject to the provisions and procedures detailed out in the Data Sharing agreement.
7. NDMO will prepare the guidelines for data sharing, which includes a request for data sharing and a standard agreement for data sharing.
8. The Regulatory Authorities, after coordination with NDMO, shall prepare the mechanisms, procedures and controls related to the settlement of disputes according to a specific time frame.
9. Whenever there is a dispute between parties involved in the Data Sharing process, each entity has the right to escalate to the Regulatory Authority - if parties belong to the same sector - to solve the dispute, or to NDMO if the dispute does not get settled or if the entities do not belong to same sector.

10. Whenever there is an aspect of sharing government data that these Interim Regulations does not cover, the entity's office can set additional controls that do not conflict with the Data Sharing principles while providing adequate justification and notifying NDMO.
11. Entities involved in Data Sharing must find the appropriate balance between the need to share data and protect data confidentiality against the potential risks to an individual or society.
12. Entitles must maintain records of Data Sharing requests and related decisions.
13. Entities should develop, adopt, and publish their internal Data Sharing policies in accordance with these Interim Regulations.
14. Once data is received, entities should not share it with any other party or entity without the consent of the Sharing Entity (SSOT).
15. Entities should be responsible for monitoring and implementing these Interim Regulations.

Freedom of Information

Interim Regulations

7. Freedom of Information Interim Regulations

7.1. Scope

This Interim Regulation applies to all requests coming from any individual to access or obtain public information – unprotected – produced or held by public entities, regardless of the source, form or nature. This includes paper records, emails, information stored on computers, audio or video cassettes, microfiche, maps, photographs, handwritten notes or any other form of recorded information.

The following information should be considered as protected, and should not be disclosed:

1. Information that, if disclosed, may harm the Kingdom of Saudi Arabia's national security, policies, interests or rights;
2. Military and security information;
3. Documents and information obtained in agreement with another state and classified as protected;
4. Inquiries, investigations, checks, inspections and monitoring in respect of a crime or violation;
5. Information that include recommendations, suggestions or consultations for issuing governmental legislation or decision not issued yet;
6. Commercial, industrial, financial or economic information that, if disclosed, may result in gaining profits or avoiding losses in an illegitimate manner;
7. Scientific or technological searches or rights included intellectual property right that, if disclosed, may result in infringement of incorporeal right;
8. Tender and bidding Information that, if disclosed, may give rise to violation of fair competition;
9. Information and the like, which are protected, confidential or personal under another law, or require certain legal action to be accessed or obtained.

7.2. Key Principles

Principle 1: Transparency

Individuals have the right to access information related to public entities' activities to enhance integrity, transparency, and accountability.

Principle 2: Accountability and Reasonable Justification

Any restrictions on requesting access or obtaining protected information received, produced, or managed by public entities must be justified in a clear and explicit manner.

Principle 3: Public Information Disclosure

Every individual has the right to access or obtain public information – unprotected – and the applicant does not necessarily have a certain status or interest in this information to be able to obtain it and is not subject to any legal accountability related to this right.

Principle 4: Equality

All the requests for access to information are treated equally and in a non-discriminatory manner.

7.3. The Rights of Individuals to Access Public Information

First: The right to access and obtain any public information – unprotected – by any public entity.

Second: The right to be informed about the reason for the denial of the request for access to information.

Third: The right to file a notice of appeal against the decision to refuse the request for access to information.

7.4. Obligations of Public Entities

1. The public entity shall be responsible for preparing and implementing policies and procedures related to exercising the right to access or obtain public information, and the entity's head is responsible for approving and adopting it.
2. The public entity shall establish an organizational unit linked to the data management offices that have been established across public entities under the Royal Decree No. 59766 dated 20/11/1439 AH, and shall assign them the responsibility to develop, document and monitor the implementation of policies and procedures approved by the top management across these entities and related to the right to access public information. The functions and responsibilities of that unit shall include development of appropriate standards to determine levels of data classification in case of their absence – according to the Data Classification Interim Regulations – and using them as a main reference while processing requests for access to public information.
3. The public entity shall determine and provide possible means (forms for requesting public information) – whether paper or electronic – through which the applicant can request access to public information.
4. The public entity shall verify the identity of individuals before granting them the right to access or obtain public information in accordance with the controls determined by the National Cyber Security Authority.
5. The public entity shall set the necessary standards for determining the fees for processing requests to access or obtain public information based on the nature of the data, its size, the effort spent, and the time taken - in accordance with the Data Revenue Framework Interim Regulation[1].
6. The public entity shall document all records of requests to access or obtain public information and the decisions taken on these requests, provided that these records would be reviewed to address cases of misuse or non-response.
7. The public entity shall prepare and document policies and procedures for proper records keeping and disposing of it in accordance with the relevant national laws and regulations.

[1] The development of the Data Revenue Framework Interim Regulations is in progress.

8. The public entity shall prepare and develop the necessary procedures to manage, process, and document the requests subject to extension or denial. They shall also define roles and responsibilities related to the appointed staff and document the cases in which the Regulatory Authority and NDMO are notified according to the time period specified for processing the requests.
9. The public entity shall notify the applicant - in an appropriate manner - in the event the request is rejected in whole or part, explaining the reasons for the denial and the right to appeal and how to exercise this right within a period not exceeding (15) days after the making the decision.
10. The public entity shall launch awareness programs to promote and enhance the culture of transparency and raise awareness of the Freedom of Information policies and procedures approved by the top management of the entity.
11. The public entity shall be responsible for monitoring compliance periodically with Freedom of Information Interim Regulation and presenting the results to the head of the entity (or the delegate). The corrective procedures should be determined in case of non-compliance and the Regulatory Authority and NDMO should be notified accordingly.

7.5. Request for Information Process

The main requirements for the request to access public information :

1. The request should be in writing or electronically;
2. The request should be filled out in a dedicated form made accessible by the public entity;
3. The request should clearly state that it is a request for Freedom of Information purposes;
4. The request should give details about how notices can be sent to the requester (for example: address, email, or through the entity's website);
5. The request should be sent directly to the public entity.

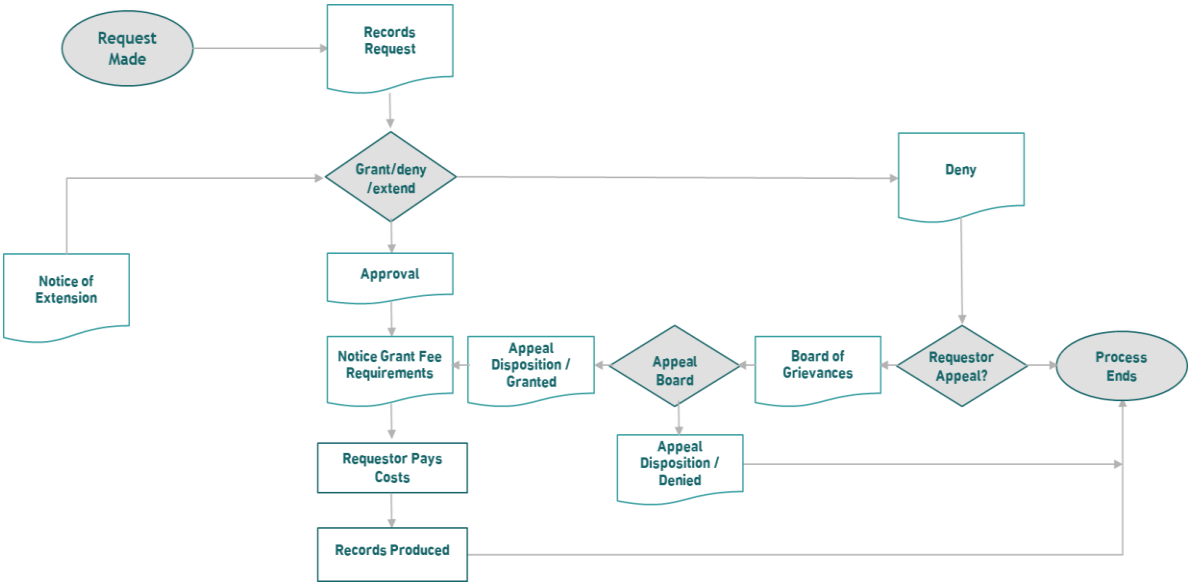

Figure 4 - Request for Information Process

The main steps for the request to access public information:

First: Applications should be submitted by filling out a "Public Information Request Form" – electronic format or paper – and submitting it to the public entity that has the information.

Second: The public entity, in not less than thirty (30) days of receipt of a request to access or obtain public information, shall take one of the following steps:

1. **Grant:** If the public entity grants a request to access to or obtain information in whole or in part, the applicant should be advised in writing the applicable fees, and the public entity should make this information available to the applicant within a reasonable period that does not exceed ten (10) days of receipt of payment.
2. **Denial:** If the public entity denies a request to access to or obtain information, rejection decision should be communicated in writing or electronically and should include the following information:
    - Whether the request is denied, in whole or in part;
    - A concise statement for the basis of denial, if applicable;
    - Notice of a right to appeal such denial, including notice as to the time and manner in which any appeal must be taken.
3. **Extension:** In the event the public entity is unable to respond to the request for access in due time, the time in which to respond should be extended within reasonable time given the size and nature of information requested – for example not exceeding an additional thirty (30) calendar days – and the public entity should provide the applicant the following information:
    - Notice of the Extension and the new date when the request is expected to be completed;
    - A concise statement for the basis of delay;

- Notice of a right to appeal such delay, including notice as to the time and manner in which any appeal must be taken.

4. **Notice:** If the required information is available on the entity's website, or is not within its competence, the individual requesting the information must be notified, in writing or electronically, including the following information:
    - The type of notice, for example, the required data is available on the entity's website, or is not within its jurisdiction;
    - The right to complain about this notice and how to exercise this right.

Third: In the event the applicant wants to appeal a denial by a public entity, they could submit a written or electronic notice of appeal to the public entity's Office within a specific period of time, not exceeding ten (10) working days after receiving the decision of the public entity. The Board of Grievances within the entity's office, shall review the application, make the appropriate decision and notify the applicant of the related fees – it is retrieved if the Board approves the request – and the appeal decision.

7.6. General Dispositions

First: Public entities shall ensure that these Interim Regulations are in line with their policies and procedures and circulate the same to all its affiliates or relevant agencies to ensure alignment and achievement of targeted objectives.

Second: Public entities shall balance between the right to be informed and to access information with other necessary requirements, such as national security and personal data protection.

Third: Public entities shall comply with these Interim Regulations and document compliance periodically, in accordance with the mechanisms and procedures determined by the entities after coordination with NDMO.

Fourth: Regulatory Authorities – in coordination with NDMO – share develop the mechanisms, procedures, and controls related to resolving complains within a specific timeframe.

Fifth: Public entities shall notify NDMO in the event the request for access to public information is rejected or the public entities have decided to extend time to respond and provide information that is in scope of these Interim Regulations.

Sixth: When contracting with other entities - such as companies performing public services - the public entity shall audit on a periodic basis the compliance of these entities according to the mechanisms and procedures determined by the entity itself, including any subsequent contracts conducted by the other entities.

Seventh: The public entities shall have the right to set additional rules for handling requests related to specific types of public information according to their nature and sensitivity after coordination with NDMO.

Eighth: Public entities shall prepare forms for the request or access to public information - whether paper or electronic – specifying the required information and clarifying possible means to provide the required information.

7.7. Freedom of Information and Open data

Open data programs and policies have been launched around the world to support growth of the national economy and innovation agenda. Making specific datasets available for public access and use has benefited researchers, innovators, other members of the public and even companies and helped create a conductive environment for business growth, promoting an open and transparent government.

Driving an open data program also represents the proactiveness of a public entity in upholding the right to access public information and making specific datasets open ahead of being requested. As such, it is expected that effective open data programs can be correlated with less Freedom of Information requests, potentially lowering government expenses.

Open data

Interim Regulations

8. Open data Interim Regulations

8.1. Scope

The scope of the Open data Interim Regulations covers all data and public information – unprotected – produced by public entities regardless of source, form, or nature. This includes paper records, emails, information stored on computers, audio or video cassettes, microfiche, maps, photographs, handwritten notes or any other form of recorded information.

8.2. Key Principles

Principle 1: Open by Default

This principle ensures that the Government avail most of its data to the public by default unless there is sufficient justification that non-disclosure of data is of greater public interest.

Principle 2: Open Format and Machine-Readable

Datasets should be made publicly accessible in a machine-readable format that allows automated processing. Data should be stored in widely used file formats (such as CSV, XLS, JSON, XML) that facilitate machine processing.

Principle 3: Up to Date

Open datasets should be regularly published in their most recent state and should be made available to the public in a timely fashion. Whenever feasible, data collected by the Government should be released as quickly as it is gathered. Priority should be given to data whose utility is time sensitive.

Principle 4: Comprehensive

Open datasets should be as complete and as granular as possible, reflecting what is recorded, in compliance with the National Data Privacy Regulation. Metadata that defines and explains the raw data should be included with explanations or formulas for how data was derived or calculated.

Principle 5: Non-discriminatory

Datasets shall be available to anyone without discrimination or requirement for registration. Any person should be able to access open data published at any time without having to identify him/herself or to provide justification for gaining access.

Principle 6: Free of Charge

Open data should be made available to the public free of charge.

Principle 7: KSA Open data License

Open data should be subject to the Kingdom's Open data License that provides the legal basis for Open data usage while defining the conditions, obligations, and restrictions applicable to the user. Any usage of Open data indicates acceptance of the License terms.

Principle 8: For Improved Governance and Citizen Engagement

Open data should enable informed civic participation and reinforce governments' transparency and accountability to improve decision-making and enhance the provision of public services.

Principle 9: For Inclusive Development and Innovation

Entities should play an active role in promoting the reuse of Open data and providing the necessary supporting resources and expertise. Entities should actively work on empowering a future generation of Open data innovators and engaging individuals, organizations, and the general public in unlocking the value of Open data.

8.3. Assessing Data Value for Defining Open datasets

The key phases for assessing data value (or the data valuation process) to enable the publication of open datasets at scale is presented as follows:

Step 1: Identifying the Data and Public Information Inventory

To assess data value, the public entity should classify data (in line with the Data Classification Interim Regulations) and identify all "publicly" classified datasets that may constitute files or tables or specific records in a database, etc. After, the benefits, applications, and potential usage for every dataset should be defined. It is possible to consider the data domain or sector when analyzing potential use cases, for example, GIS data can benefit the health sector. In addition, it is possible to consider data sources: data collected from users directly, data automatically collected through recorded events such as electronic transactions, aggregated data, or data developed from combining data, etc.

Step 2: Assessing Data Value

After identifying the datasets in the previous step, the main factors related to the usefulness of the data are analyzed which play a critical role in assessing its value, such as data completeness, accuracy, consistency, timeliness, restrictions, exclusivity, potential risks from publication, or ability to access and integrate with other data.

Step 3: Identifying Potential Stakeholders

After assessing the data value in the previous step, potential stakeholders are identified whether entities or individuals across the value chain, for example, it is possible to publish consumer trends to product manufacturers not just to department stores. Therefore, it is important to understand the key drivers for stakeholders, whether for example it relates to generating revenue by developing data products or implementing services for the public benefit such as for improving quality of life.

After the data valuation process, the open data lifecycle may starts as described in what follows.

8.4. Open data Rules and Obligations

The Open data Regulation defines rules and obligations that Adopting Entities should comply with throughout the Open data Lifecycle comprising:

- Open data planning
- Open data Identification
- Open data Publishing
- Open data Maintenance
- Open data Performance Tracking

Open data planning

The public entity shall:

1. Establish the role of an Open data and Information Access Officer in the entity's data management office with the primary responsibility to support the planning, execution, and reporting of the entity's Open data agenda and in compliance with these Interim Regulations.
2. Develop an Open data plan that shall include the following:
    - Key strategic objectives for Open data at the entity level
    - Identification and prioritization of the entity's datasets to be published on the National Open data Portal
    - Open data KPIs and targets for the entity
    - Prioritization methodology and criteria
    - Training needs related to Open data
    - Timelines for Open data publication and maintenance.
3. Develop and document the processes required across the lifecycle of Open data, including but not limited to:
    - Processes to identify public datasets to be published by the public entity
    - Processes to validate and systematically review the compliance of Open data with security, privacy, and quality-related requirements and to immediately address any identified concern
    - Processes to ensure that datasets are published and maintained to their appropriate format, timeliness, comprehensiveness, and overall high quality and ensure the exclusion of any restricted data
    - Processes for gathering feedback, analyzing performance at the Entity level, and improving the overall Open data national impact.
4. Ensure the Open data plan is reviewed and maintained periodically.
5. Submit an annual report to NDMO on the Open data plan and progress towards the Open data targets and as defined in the Plan.

6. Conduct training related to Open data with support or coordination with NDMO.
7. Perform awareness campaigns to ensure potential users are aware of the existence, nature, and quality of the Open data offered by the entity.

Open data Identification

The public entity shall:

1. Regularly and systematically identify all data classified as "Public" and evaluate the priority for publication as Open data for each dataset identified.
2. Assess the value and priority for publication of a dataset when receiving a request for publication, or whenever a previously restricted dataset is declassified as "Public".
3. Capture and duly populate the metadata for the identified Open datasets.
4. Consider whether some combination of any publicly available data and the data intended to be published could allow for the identification of an individual or create any other security or privacy risk or threat.

Open data Publishing

The public entity shall:

1. Publish their Open datasets on the official National Open data Portal.
2. Ensure that data is published in discoverable, well-structured, machine-readable, non-proprietary, standardized data formats, including but not limited to: CSV, JSON, XML, and RDF. The dataset files shall be accompanied by documentation related to the format and instructions on how to use them.
3. Whenever possible and applicable, provide data in multiple formats.

Open data Maintenance

The public entity shall:

1. Ensure all published Open datasets are updated regularly as per the frequency defined in the metadata.
2. Perform continuous review of the published Open datasets to ensure they meet defined regulatory requirements.
3. Ensure that metadata is updated and maintained whenever data elements of the published Open datasets change.
4. Maintain data traceability by documenting data provenance and maintaining versioning history of the dataset.
5. Publish Open datasets with quality limitation statements clearly defined, documented, and stated in the Metadata.

Open data Performance Tracking

The public entity shall:

1. Analyze the demand, download, and usage of its Open data to understand public demand and reprioritize datasets accordingly.
2. Collect, analyze and timely respond to users' requests received directly or through the National Open data Portal for the publishing of additional datasets.

8.5. Roles and Responsibilities

The Open data Interim Regulations define the following roles and responsibilities both at the national and entity level.

National Level

1. NDMO

NDMO – with the responsibility of overseeing open data initiatives in the Kingdom – shall coordinate Open data activities at the national level. It shall provide the KSA Open data strategic direction and develop the national regulations, standards, and guidelines to ensure Open data is effectively managed and published across the Kingdom and yields the targeted national impact.

As such, NDMO's responsibilities shall include:

- **Open data Regulation Development** - Develop, issue, and update the Open data Regulations (in line with these Interim Regulations) to be revisited yearly to address possible changes affecting the Open data lifecycle.
- **Open data Adoption Plan Development** - Develop supporting material and provide continuous guidance to entities to facilitate the adoption of Open data Interim Regulations.
- **Open data Advisory** – Support entities in complying with these Interim Regulations and answer any queries related to the Open data lifecycle.
- **Open data Compliance Measurement** – Measure compliance of entities on a yearly basis based on the defined compliance mechanism (Refer to the 'Compliance' section for more details) and audit Open data activities when required.
- **Open data Education and Awareness** – Conduct and monitor communication and training initiatives to drive Open data awareness and adoption at the national level.
- **Open data Consolidation** – Consolidate and maintain the list of available Open datasets at the National level to monitor and report on progress.
- **Open data Performance** – Analyze Open data usage and impact at a national level and synthesize improvement opportunities to be communicated to relevant stakeholders.
- **Developing and Maintaining the Open data License** – Develop the KSA Open data License to allow users to use, share, and modify the open data and maintain it as needed.

2. National Information Center (NIC)

NIC shall act as the technical operator of the National Open data Portal including the design, build, operations and maintenance of the platform.

As such, NIC's responsibilities shall include:

- **Manage National Open Data Portal** – Design, build, and maintain the National Open data Portal to ensure entities can publish, manage, and update their open datasets.
- **Authorize and Guide Portal Participation** – Authorize entities and ensure they have appropriate access to the National Open data Portal. Develop operational and technical guidelines for publishing and maintaining Open data on the National Open data Portal.
- **Capture Portal Usage Trends** – Capture usage trends and statistics across published Open data and provide them to NDMO and entities.

Entity Level

All entities shall have the primary responsibility for ensuring their Open data is being published in compliance with the Open data Interim Regulations. As such, entities shall designate individuals who will be responsible for carrying out the Open data activities as outlined below.

The main responsibility for the Open data activities within the entity lies with the Open data and Information Access Officer.

Head of the Entity - The head of the Entity – or as delegated – is accountable for the Open data practice within the entity, responsibilities include:

- **Open data plan Approval** – Approve and oversee the implementation of the Open data plan within the entity.
- **Open data Roles Assignment** – Designate different roles with regards to Open data.
- **Open data Yearly Report Approval** – Approve the Open data annual report prepared by the head of the entity's data management office.

Head of the Entity's Office - Considered the strategic lead of the Open data practice. Responsibilities include:

- **Open data Strategic Planning** - Oversee the development of the Open data plan and present it to the head of the entity; also review the performance of Open data to identify improvement opportunities and feed into the Open data plan.
- **Open data Supervision** – Review the Open data identification and prioritization activities, approve Open data publication, and ensure Open data maintenance activities are being performed.
- **Open data Compliance** – Ensure compliance of the entity's Open data activities with national regulations, including but not limited to Data Classification, Data Privacy, and Freedom of Information.

- **Point of Contact for NDMO** – Act as the first point of contact between the entity and the NDMO. The head of the entity's office shall resolve any pending issues around Open data for their respective entity and escalate them to NDMO whenever necessary.

Open data and Information Access Officer (ODIAO) - The ODIAO is the operational lead of Open data within the entity. Responsibilities include:

- **Open data planning** – Develop the Open data plan, including the Open data prioritization methodology, and set targets and KPIs to be agreed on with the head of entity's office and head of the entity.
- **Open data Management** - Manage Open data activities within the entity, in particular:
  - The identification of Open data
  - The prioritization of datasets publication
  - The preparation of datasets for publication and the documentation of metadata
  - The publication of Open datasets on the National Open data Portal
  - The update, maintenance, and quality review of published datasets.
- **Open data Requests Consolidation –** Review Open data feedback relevant to the entity and record and consolidate requests to publish specific data as Open.
- **Open data Education and Awareness -** Educate and raise awareness across Entity's employees on Open data and support national awareness campaigns in coordination with the head of the entity's office.
- **Point of Contact for NDMO (Secondary) –** Act as the secondary point of contact between the entity and NDMO.

Business Data Executive (BDE) - The Business Data Executive has the following responsibilities:

- **Endorse the Open data plan** – Contribute to the development of the Open data plan and manage the teams to implement the Plan in coordination with the ODIAO.
- **Open data Prioritization** – Advise the ODIAO on the value of public datasets and the investments required to publish and maintain them.
- **Datasets Review and Approval** – Review and approve the datasets to meet the Regulation specifications in terms of quality, completeness, and metadata documentation before submitting them for publication.

Business Data Steward (BDS) - The Business Data Steward is a member of the BDE team responsible for:

- **Open datasets Identification -** The BDS shall systematically review and identify the data created and processed by its department and if needed, classify it as public.
- **Open datasets Preparation –** Prepare the Open datasets to be published to meet the Regulation specifications in terms of quality, completeness, and metadata documentation before submitting them for publication.
- **Open datasets Maintenance –** Update and maintain published Open datasets and related metadata.

8.6. Compliance

NDMO, as the national regulator of the data agenda, shall monitor compliance against the Open data Interim Regulations with the support of the Regulatory Authorities.

Compliance Terms

1. All public entities shall abide by the Open data Interim Regulations and submit a report to NDMO on an annual basis covering, but not limited to:
   - The progress of the entity against the defined entity Plan
   - The targets and KPIs set in the Open data plan
   - The number of open data sets identified
   - The number of open data sets published
2. Regulatory Authorities – in coordination with NDMO – shall develop the mechanisms, procedures, and controls to resolve disputes related to Open data publication.
3. NDMO shall review the annual reports submitted by public entities with regards to their compliance against the Open data Interim Regulations and share them with relevant entities.
4. NDMO is entitled to initiate ad-hoc or periodic compliance audits on any public entity and conduct a review of each decision to publish or refuse to publish data.

Non-compliance Response

When responding to non-compliance, NDMO shall adopt a gradual approach based on the understanding of the reason for non-compliance and its severity. Accordingly, there are three levels of responses:

- **Education** – NDMO shall focus on education when dealing with accidental or non-intentional non-compliance with minor negative impacts.
- **Co-operation** - NDMO shall co-operate to prevent, deter, or address non-compliance with moderate negative impacts that is careless or opportunistic in nature.
- **Direct interventions** – NDMO shall investigate ongoing and repetitive non-compliance or those with high negative impacts.