Governance policies

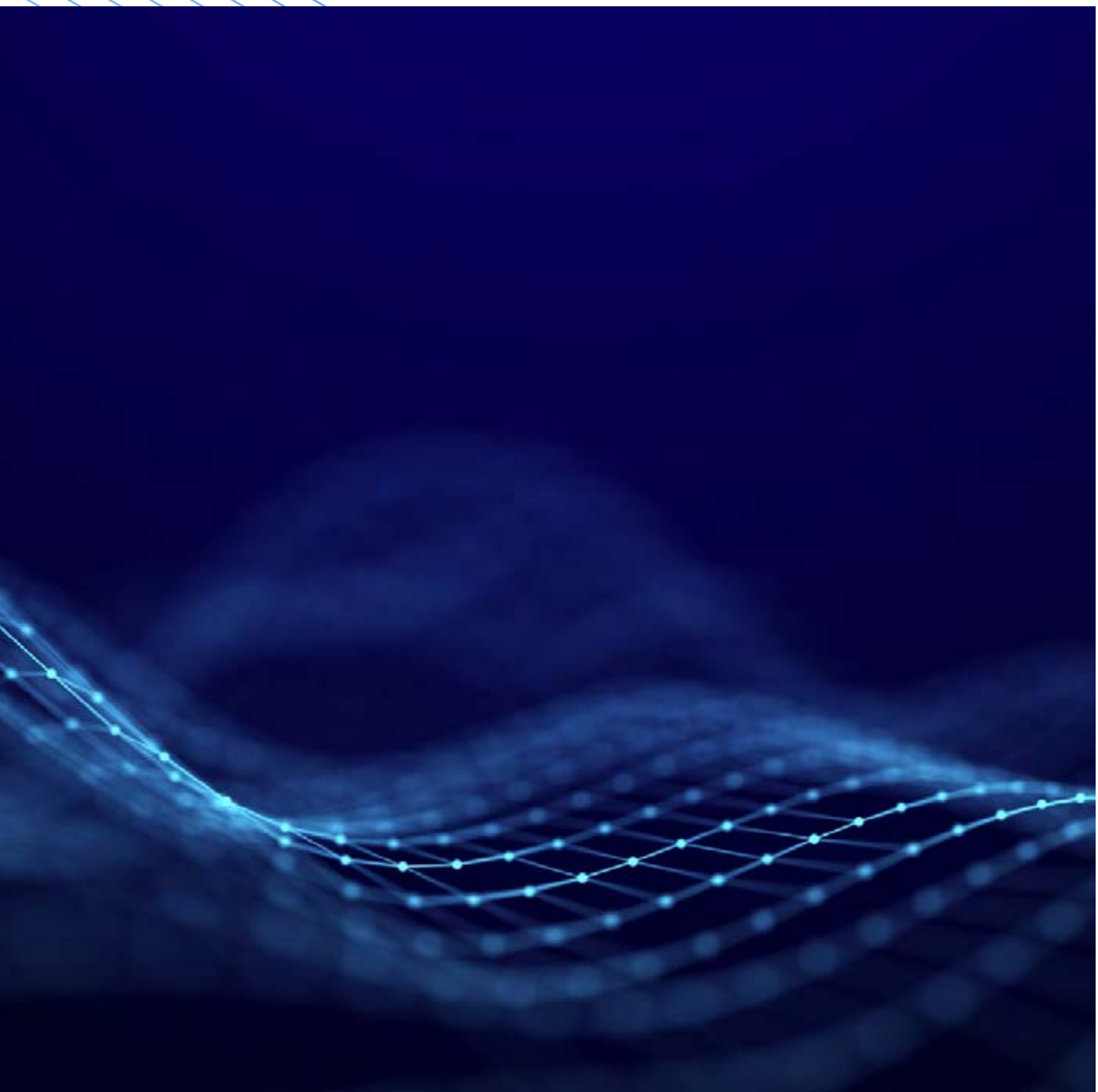
National data

Second Edition

Date: 05/26/2021


بسم الله الرحمن الرحيم

Contents




661.455
807.100
244.521
456.487

1. Introduction

Data produced, received, or handled by government agencies represent national assets that can contribute to improving performance and productivity and facilitating the provision of public services by supporting effective data management processes, making strategic decisions, anticipating the future, and achieving the highest levels of accountability and transparency. Countries around the world are also seeking to benefit from the value of data as an economic resource that helps innovation, contributes to supporting economic transformations, and enhances countries' competitiveness. At the national level, government agencies collect and process huge amounts of data that can be used to contribute to economic growth and advance the Kingdom to leadership among data-driven economies.

To ensure maximum benefit from this data, which constitutes an important part of national assets, it is necessary to strengthen the principle of data sharing to achieve integration between government agencies and reduce data duplication, conflict, and multiple sources. This requires classifying data into unified levels that help achieve a balance between the advantages and risks of data sharing between agencies in the public and private sectors, as well as the third sector, as data classification is considered a barrier. The angle for organizing the process of publishing open data, making public information available, and exchanging protected data, including personal data. This, in turn, helps raise the level of community oversight standards over the performance of public entities, increase the level of transparency, enhance integrity, and remove unnecessary secrecy from the activities of public entities by regulating the exercise of the right to view or obtain public information.

With the steady development of technology and the ease of obtaining and sharing data, the importance of maintaining the privacy of personal data is multiplied, which has prompted most countries to enact systems and legislation that regulate the collection, processing, and sharing of personal data, ensuring the preservation of the privacy of the owners of this data and the protection of their rights, as well as preserving national digital sovereignty over this data.

Under Vision 2030, the Kingdom is striving toward a new era that enhances the performance of government agencies, increases their transparency and accountability, and encourages economic diversification and the use of data-driven services, all of which play a significant role in a global economy built on trust and international partnerships.

Based on this, the National Data Management Office – in its capacity as the national data regulatory body – has developed a temporary framework for data governance at the national level that defines policies for data classification, data sharing, regulating the collection and processing of personal data, and how to exercise the right to access or obtain public information from government agencies, and open data until the issuance of regulations and legislation related to data classification, data sharing, personal data protection, and freedom of information. In addition to these systems and legislations, the Office decided to combine the policies related to them into one document that clarifies the extent of the relationship and dependence between them, as shown in Figure 1 below.

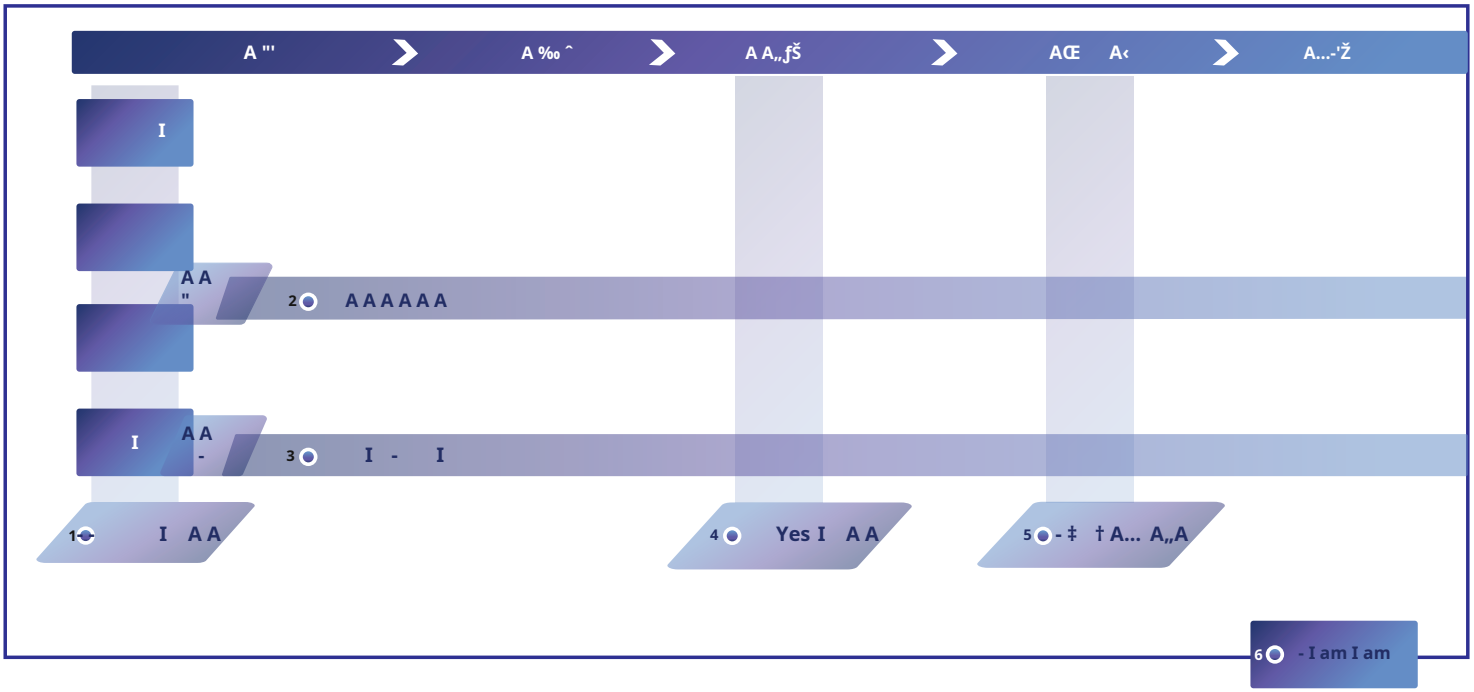


Figure 1: The relationship between data regulations, legislation, and policies

2. Definitions

For the purposes of implementing these policies, the words and terms mentioned below - wherever they appear in this document - shall have the meanings indicated opposite each of them, unless the context requires otherwise:

Personal data:

Every statement - regardless of its source or form - It is likely to lead to identifying the individual specifically, or make him directly or indirectly identifiable when combined with other data, and this includes:
- For example, but not limited to - name, personal identification numbers, addresses, contact numbers, bank account and credit card numbers, still or moving images of the user, and other data of a personal nature.

Data:

A collection of facts in their raw form or in an unorganized form such as numbers, letters, still images, video, audio recordings, or emojis.

Data access:

The ability to have logical and physical access to the entity's data and technical resources for the purpose of using them.

Data access level:

A level based on permissions and authorities that restrict access to data and technical resources to authorized persons according to what is required to accomplish the tasks and responsibilities assigned to them.

Verification:

Verifying the identity of any user, process or device is a prerequisite for allowing access to technical resources.

Statement:

Defining the rights and permissions to access data and technical resources for any user, program, or process, and controlling the levels of access to them.

Data availability:

Ensure appropriate and reliable access to and use of data when needed.

Data confidentiality:

Maintaining authorized restrictions on access to or disclosure of data.

Data security:

Protect data from any unauthorized modification or destruction.

Protected data:

Data classified as (Top Secret, Confidential, Restricted).

General information:

Unprotected post-processed data received, produced or handled by public bodies, regardless of its source, form or nature.

Open data:

A specific set of public information – machine-readable – that is freely and unrestrictedly available to the public and can be used or shared by any individual or public or private entity.

Sensitive data:

Data whose loss, misuse, unauthorized access, or modification would cause serious harm or negatively impact national interests, the activities of government agencies, or the privacy of individuals and the protection of their rights.

Data classification levels:

The following classification levels: (Top Secret), (Confidential), (Restricted), (General).

Individual:

The person who requests to view or obtain public information.

Personal data holder:

The natural person to whom the personal data relates, or his representative or the person who has legal guardianship over him.

Processing of personal data:

All operations conducted on personal data by any means, whether manual or automated. These operations include, but are not limited to, collecting, transferring, preserving, storing, sharing, destroying, analyzing, extracting patterns, drawing conclusions from them, and linking them with other data.

Control side:

Any governmental entity or independent public legal entity in the Kingdom, and any private natural or legal person; determines the purpose of processing personal data and how it is done, whether the data is processed by it or by the processing entity.

Processor:

Any governmental body or independent public legal entity in the Kingdom, and any private natural or legal person, that processes personal data for the benefit of and on behalf of the controlling body.

Disclosure of personal data:

Enabling any person - other than the controlling authority - to obtain, use or access personal data by any means and for any purpose.

Personal data leakage:

Disclosing, obtaining, or enabling access to personal data without authorization or legal basis, whether intentionally or unintentionally.

Implied consent:

It is a consent that is not explicitly granted by the data subject, but is implicitly granted through the person's actions and the facts and circumstances of the situation, such as signing contracts or agreeing to terms and conditions.

External parties:

Any governmental body or independent public legal entity in the Kingdom, and any private natural or legal person other than the data owner, the controller, the processor, and authorized persons, that is concerned with processing personal data.

Business Data Representative:

He is the person responsible for the data collected and maintained by the public entity in which he works. He is often at a high administrative level, and there may be more than one business data representative in the public entity.

Data User:

Any person granted access to the data for the purpose of viewing, using or updating it in accordance with the tasks authorized by the Business Data Representative.

Metadata:

It is the information that describes data and its characteristics, including business, technical and operational data.

Machine-readable data:

It refers to structured data in a specific format that can be read and processed automatically using computers, tablets, and other devices.

Processor:

Any governmental body or independent public legal entity in the Kingdom, and any private natural or legal person, that processes personal data for the benefit of and on behalf of the controlling body.

National Open Data Platform:

It is a unified national platform at the Kingdom level concerned with managing, preserving, and publishing open data sets.

Open Data License:

A license regulating the use of open data.

Open formula:

Any widely accepted, non-proprietary, non-platform-specific format that is machine-readable, enables automated processing of such data, and facilitates analysis and research capabilities.

applicant:

Any entity from the public, private, or third sector, or any individual who submits a request to share data.

Data sharing request:

The form for requesting data sharing, which includes information about the requester, the data requested, and the purpose for which the data sharing was requested.

Data Sharing Agreement:

An official agreement signed between two parties - a government agency and any other party - to agree to share data according to specific terms and conditions that are consistent with the principles of data sharing.

Data sharing mechanism:

The method by which data is shared - including the means of transmitting the data, the parties involved in sharing the data, and the sharing model: direct sharing, sharing via a service provider, sharing via multiple parties.

Security controls:

The devices, procedures, policies and physical safeguards used to ensure the integrity and protection of data and the means of processing and accessing it.

Public Authority:

Any governmental body or independent public legal entity in the Kingdom, or any of its affiliated entities. Any company that manages, operates or maintains public facilities or national infrastructure, or provides a public service in relation to the management of such facilities or infrastructure, shall be considered a public body.

Regulatory Authority:

Any governmental body or independent public legal entity that undertakes regulatory or supervisory tasks and responsibilities for a specific sector in the Kingdom of Saudi Arabia based on a legal document.

Office of the region:

Data Management and Privacy Office in the public authority.

Office:

National Data Management Office.

The child:

Every person who has not exceeded eighteen years of age.

Eligibility:

The person’s authority to issue actions in a manner that is legally and legally recognized.

Incompetent:

Someone with incomplete capacity, such as a special minor - He is the one who has completed the age of seven but has not completed the age of eighteen - and the heedless, the foolish, the one who has a mental disability, and the like.

And those in the same position: those who lack or are partially legally competent.

Guardian:

One of the parents or whoever has guardianship over the child's affairs according to the provisions of Sharia or relevant regulations.

State:

An authority established by Sharia for the guardian, granting him the power to act and manage the child's affairs on his behalf with regard to his body, soul, and money, and to achieve his interests, including making decisions regarding the processing of his personal data.

Sensitive personal data:

Any personal data that includes a reference to the child's or someone similarly racial or tribal origin, or his or her religious, intellectual, or political beliefs, or indicates his or her membership in civil associations or institutions, as well as criminal and security data, biometric data that determines identity, genetic data, credit data, health data, location data, and data that indicates that the individual's parents or one of them are unknown.

Privacy Notice:

It is an external statement directed to individuals that explains the content of personal data, the means of collecting it, the purpose of processing it, how it will be used, the parties with whom this data will be shared, the period for which it will be retained, and the mechanism for disposing of it.

privacy policy:

It is an internal document directed to employees in entities that clarifies the rights of data owners and the obligations that must be complied with to preserve the privacy of data owners and protect their rights.

Data Disclosure:

Enabling any person - other than the controlling authority - to obtain, use or access personal data by any means and for any purpose.

Transfer of personal data:

Sending personal data to a party outside the geographical borders of the Kingdom - by any means - for the purpose of processing it, whether directly or indirectly, in accordance with specific purposes based on regulatory foundations, including transfer for security purposes, to protect public health or safety, or in implementation of an agreement to which the Kingdom is a party.

Express consent:

Written or electronic consent that is explicit, specific, and issued with the free and absolute will of the data subject, indicating his acceptance of the processing of his personal data.

Direct marketing:

Any communication, by any means, through which marketing or promotional material is directed to a specific person.

Live broadcast:

Transferring personal data from the sending party to the receiving party without the data passing through any other party.

Indirect transport:

Transferring personal data from the sending party to the receiving party, through one or more other parties.

Transverse transport:

Transferring personal data on an infrequent or irregular basis – usually a one-time basis – to a limited number of persons, including, for example, transferring data for the purpose of benefiting from a service in another country for the benefit of the data owner.

Accreditation List:

A list approved by the National Data Management Office that includes the names of countries that have an adequate level of protection for the rights of data subjects with regard to the processing of their personal data.

Control side:

Any governmental entity or independent public legal entity in the Kingdom, and any private natural or legal person; determines the purpose of processing personal data and how it is done, whether the data is processed by it or through the processing entity.

Processor:

Any governmental body or independent public legal entity in the Kingdom, and any private natural or legal person, that processes personal data for the benefit of and on behalf of the controlling body.

Unprocessed data:

It is the data that has not been subjected to advanced processing operations and is exchanged in its raw form, such as the basic data of the citizen that is displayed on the national identity card, with the exception of the processing imposed by systems, regulations and policies for the purpose of sharing data, including, but not limited to, prior processing before sharing personal data, such as masking data, scrambling or data anonymization.

Data Products:

Services or applications based on data after processing it with the aim of creating added value by integrating it with other data, enriching it, adapting it, analyzing it, or representing it, including, but not limited to: predictive or descriptive insights and analytics, interactive dashboards (platforms), and others.

Data Monetization:

Converting the intangible value of data into real or physical value directly (by providing raw data) or indirectly (by offering data products).

Revenue Generation Model:

The entity's revenue stream management strategy, the resources required for each revenue stream, and the target consumers.

Business model:

The framework that describes how market value can be created by exploiting business opportunities, including key partners, key activities, customer segments, revenue model and revenue streams, and clarifies the logical links between them and how they work together.

Pricing Model:

The mechanism used to determine the intrinsic value (price) of data and data products.

Government data:

It is the data produced by government agencies.

Government services:

Basic services provided by government agencies, which can be provided by a third party on behalf of the government agency.

Data provider:

Any individual, government entity, or private entity that provides data or offers data products for financial compensation, directly or indirectly.

Data beneficiary:

Any individual, government agency, or private entity that requests data or benefits from data products in exchange for money.

Marketing:

The activity of exchanging, trading or supplying raw or processed data in exchange for a cash amount or other in-kind value.

Government agency:

Any governmental body or independent public body in the Kingdom, or any of its affiliated bodies. Any company that manages, operates or maintains public facilities or national infrastructure, or provides a public service in relation to the management of such facilities or infrastructure, shall be considered a governmental body.

Private entity:

Any private legal entity licensed to operate in the Kingdom - whether local or foreign - and the individual, whether a citizen or an official resident in the Kingdom, who provides data or presents data products is considered a private entity.

Non-profit organization:

Any non-governmental entity licensed to operate in the Kingdom and provides its services and products on a non-profit basis.

Developer:

Any natural or legal person that develops artificial intelligence systems by building predictive models using data and algorithms to achieve specific goals.

user:

Any natural or legal person who applies or uses artificial intelligence systems to achieve specific goals.

Data owner:

The individual to whom the personal data relates, or his representative or legal guardian.

Sample data:

Data used to build, train, and test predictive models and artificial intelligence algorithms to achieve specific outcomes.

Artificial intelligence technologies:

It is a set of predictive models and advanced algorithms that can be used to analyze data, forecast the future, or facilitate the process of making decisions about expected future events.

Facial recognition technologies:

Technologies that enable the analysis of key facial features (biometrics) to determine the personal identity of individuals in still or moving (visual) images.

3. Objectives

With reference to the text of Cabinet Resolution No. (292) dated 04/27/1441 AH, which stipulates in paragraph (1) of Article "Tenth" that the Office shall undertake to develop policies, governance mechanisms, standards and controls related to data and artificial intelligence and follow up on compliance with them after their approval, accordingly, the National Data Management Office has benefited from international practices and standards when developing policies related to national data governance, which aim to:

1. Support and enhance the Kingdom's efforts to achieve the national vision and strategies.
2. Promote a culture of data sharing and collaboration to enhance and develop data, information, and knowledge assets.
3. Regulating the dissemination, exchange and use/reuse of protected data and public information.
4. Achieving integration between government agencies.
5. Enabling government agencies to prepare their policies, implement their plans, and anticipate the future.
6. Maintaining the privacy of personal data and the confidentiality of sensitive data.
7. Preserving the rights of individuals when dealing with personal data and public information held by authorities Governmental.
8. Promoting the concept and practices of open data to improve transparency among public entities and encourage Research, innovation and driving economic growth.
9. Enhancing transparency and establishing governance rules by distributing roles and responsibilities.
10. Preserving national digital sovereignty of personal data.
11. Raising the level of community oversight standards for the performance of public entities.
12. Support efforts to enhance integrity and combat corruption through access to public information as a human right. guaranteed.
13. Enabling entities to invest and innovate in services based on personal data to enhance Developmental, economic and competitive gains that contribute positively to raising the Kingdom's gross domestic product.
14. Raising the level of trust in data-driven services.
15. Raising the level of electronic services and transactions to achieve integration.
16. Contributing to raising the level of commercial and economic performance through transparency and fair access to information. Public to enhance competitiveness and equal opportunities.

17. Advancing scientific research by encouraging researchers to benefit from general information and advance The developmental and supervisory role of society and its institutions.

18. Providing equal opportunities for those seeking general information, which contributes to promoting equal citizenship. And partnership in raising awareness of the general issues of the country.

4.Private Policies

National Data Governance

To contribute to raising the level of maturity in the field of data and artificial intelligence, seven national data governance policies were launched:

Data Classification Policy

Protecting the confidentiality of national data and classifying it at four levels.

Personal Data Protection Policy

Regulating the process of collecting, processing, and sharing personal data and preserving national digital sovereignty over it.

Data Sharing Policy

Enhancing data sharing to achieve integration between government agencies and obtaining data from their sources.

Freedom of Information Policy

Regulating beneficiaries' access to or access to public information in all its forms from government agencies.

Open Data Policy

Making open (unprotected) data and information available to all beneficiaries.

Personal Data Protection Policy for Children and Those in Their Care

Assisting relevant authorities in protecting children and those in their care from potential risks (violence, abuse, assault, threats, harm, or exploitation) resulting from the collection and processing of their personal data through websites and digital applications.

General rules for transferring personal data outside the geographical borders of the Kingdom

Maintaining national digital sovereignty over personal data and working to provide the highest levels of protection when transferring personal data outside the Kingdom's geographical borders to ensure the preservation of the privacy of its owners and the protection of their rights.

Data Classification Policy

4.1. Data Classification Policy

4.1.1. Scope

The provisions of this policy apply to all data received, produced, or handled by public entities, regardless of their source, form, or nature. This includes paper records, meetings, communications via social media and applications, emails, data stored on electronic media, audio or video tapes, maps, photographs, manuscripts, handwritten documents, and any other form of recorded data.

4.1.2. Main principles of data classification

The first principle: the origin of data is availability.

Data should be available (in the development field) unless its nature or sensitivity requires higher levels of classification and protection, and highly confidential (in the political and security field) unless its nature or sensitivity requires lower levels of classification and protection.

The second principle: necessity and proportionality

Data are classified into levels according to their nature, level of sensitivity, and degree of impact, taking into consideration the balance between their value and degree of confidentiality.

Principle 3: Timely Classification

Data is classified when it is created or when it is received from other parties, and the classification occurs within a specific period of time.

Principle 4: The highest level of protection

The highest level of classification is adopted when the content of an integrated set of data includes different levels of classification.

Principle 5: Separation of Duties

The duties and responsibilities of employees - with regard to data classification, access, disclosure, use, modification or destruction - shall be separated in a manner that prevents overlap of jurisdiction and avoids the dispersion of responsibility.

Principle 6: The Need for Knowledge

Access to and use of data is restricted on a need-to-know basis, and to the smallest possible number of employees.

Principle Seven: Minimum Privileges

Employee privilege management is restricted to the minimum privileges necessary to perform the tasks and responsibilities assigned to them.

4.1.3. Data classification levels

Table (1) below shows the main levels of data classification in accordance with the level of impact, and also shows some guiding examples for each level.

level Classification	degree of impact	Description	Examples of guidance Adia
	High	It is preserved The data is as follows: **Top Secret Data** If unauthorized access to this data The official or disclosure of its contents leads About her or Ato serious harm that cannot be And an exception remedied or repaired: ● The interests National security, including breach By agreement of treaties or causing harm By hearing And the Kingdom or diplomatic And belonging relations, political, security, military For practical purposes or economic operational efficiency Homeland Y Or national infrastructure or Government businesses. ● Performance of Bring the public what causes harm With serum H Nationalism. ● Health no Individuals and their safety on a wide scale Especially S Senior officials. ● Resources Environmental or natural.	● Plans And the details of the operation Military or Any con- Relevant blame And it has it ● Information MAt The politician Official website The learner Q ō With a relationship T International And the agreement Qat or the treaty T And everything related It has m N Discussions and studies S Works and deeds Preparation -a ● The teacher and at is related to Security shock And measures the formations of the No way T Expertise and equipment hA. ● Information M Related to the to erses and keys gloating user's opinion to nfrastructure The National And ● Announced MAt The case Terrorism for Oh my God T Tat The threatened security. ● Information Mrelated matters Weapons and ammunition Or the pain and litary reality For defensive Any m S from security strategy or strength And the satire sources. ● Information About the movement of Forces The Muslim H the characters, or the S The other ball, Or investigate forces of the actors A o the head. ● Information It affects the sovereignty of the state And it is
secret	**middle**	It is classified as For data as **"Confidential data"** If The description was unauthorized access to this data Or disclosure or its contents causes harm: Body to ● The interests Nationalism is like causing partial damage. By hearing And the Kingdom and diplomatic relations, Or the palm operational efficiency of security operations, The military Y national economy or infrastructure Infrastructure National and government business. ● It happens K Financial Sarah at the organizational level for It leads to bankruptcy or inability of entities to perform or His tasks a serious loss of competitiveness or both Both ● Causes In the event of serious harm or injury On the neighborhood affecting a group of individuals.	● Information at About Sites Material storage Logis Tia or Warehouses Economic. ● Information T Related to the origin T Vitality. ● Reminder T Understanding With the Sh International companies To create interests Commercial Or economic My strategy Coming to the Kingdom. ● Information related to machines FBinary values And a reminder T Diploma of Understanding S Between the Kingdom and countries The other.

level Classification	degree of impact	Description	Examples of Esther ShAdia
	middle	• Perform to long-term damage to resources Environmental And natural. • Investigation In major cases defined by the system, As my case financing terrorism.	
restricted	**low**	It is manufactured F Data is considered “restricted” if Description to unauthorized access to, or disclosure of, Disclosure the data or its content would result in: • Impact Limited negative impact on the work of General entities or economic activities in the On A Kingdom or on a specific person. • Harm M Limits on the assets of any entity and the loss of Mahdo this on its financial and competitive position. • Harm M Short-term limits on resources or natural Environmental And resources.	• known Do not harm anyone's reputation. Public figure • Data Detailed transactions Individualism. • Results Research and studies T The process before Publish it A. • Information Matt related to Products under Development -r which may harm Fair competition. • known Issues related to education Y Girls and decisions Administrative Sensitive. • known The health file for no Individuals • known Identity determination And like a name And the current And ID numbers National and numbers Phones F And numbers Al-Hasa Bat and licenses And our statement T Features Vital -a. • known Employee salaries N. • Documents Like the plans of the touch Planning Twi And programs C Marketing comes before Sh About him to the public And a line T technical creativity. • Contracts M Roses and offers A Show them. • Requests Make presentations. • Communications F New product before Put it to the public. • Details For design and implementation Q security systems (c-d-ar) To protect and control the S And plans The network And others. • political Devices and procedures T Interior Messages / Internal notes. • Lists Internal phones Mailing lists Electron and Harm for some C Give it to me.

level Classification	degree of impact	Description	Examples of Esther ShAdia
	nothing	It is manufactured F Data is considered “public data” when It does not depend on unauthorized access to it is granted. Statement T Or disclose it or its content, any of the above The effects mentioned, in the event that there is no effect On M t comes: • pas S National Council • incl Ti and the authorities • I am a los For individuals • The Moa Environmental response	• crowne h National Strategic Plans Announced. • The Ihda S Nationalism H a Fo population Walby Class and works according to For industry and others. • Developme General and academic T Economic. • Procedu and government and policy Tha. • I am no and related to the cheek M general information that appreci this is the government for the citizen Yen. • Jaha T Contact in the institution Sat. • Advertisem I have jobs. • Advertisem General information. • Insist Y ournalistic stories. • Results C Financial statement announced to the public aRd • A rd D Products (general). • I am no and Public Relations Matt And • any M Publicly available On any sites I agree S information. • The adve Nat.

Table 1: Data classification levels

The first principle: the origin of data is availability.

Data classified at a restricted level can also be classified into sub-levels based on the scope of the impact as follows:

Restricted - Level (A): If the scope of the impact is at the level of an entire sector or general economic activity.

Restricted - Level (B): If the scope of the impact is at the level of the activities of several parties or interests A group of individuals.

Restricted - Level (C): If the scope of the impact is at the level of the activities of a single entity or the interests of a particular individual. The table below explains and specifies the correct classification level that enables entities to assess the degree of impact resulting from unauthorized access to data or disclosure of it or its content (for more information about the impact assessment process, you can see “Steps required for data classification”).

Each party must conduct its own impact assessment of unauthorized access or disclosure, and this list is not exhaustive.

Main impact category	national interest
Sub-category of impact	Kingdom's reputation
Considerations	Will the information be subject to local or international media attention? Will it give a negative impression? Y?

Impact level			
S very watery	secret	restricted	general
Ato	middle	low	No trace
Reputation is greatly affected.	Reputation is affected to some extent.	Reputation is not affected.	No effect At have interests Homeland Vitality Yes.

Main impact category	national interest
Considerations	Does the information pose a threat to relations with friendly countries? Will it escalate tensions? International? Could it lead to protests or sanctions from other countries?

Impact level			
Top Secret	secret	restricted	general
High	average T	LowD	No, no C D effect
Severing diplomatic relations and political affiliations or threatening agreements and treaty terms, or both	Affected by Diplomatic relations negatively AFor the long term	He will not - It has an impact Relationships on diplomacy or It will limit Th Simple effect on The range Short	No, no Cd impact on national Animal Yinterest.

Main impact category	national interest
Sub-category of impact	National economy
Considerations	Does disclosure of information lead to economic losses at the national level?

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
Long-term impact on the national economy with an irreversible decline in the gross domestic product, financial market prices, unemployment rate, purchasing power, or other relevant indicators, which will negatively impact all sectors in the Kingdom.	Long-term impact on y On the national economy N educe with a manageable y-aur s in decline in GDP And the percentage Unemployment, financial S Waq prices or the general Visionary; power, which negatively y sector affects one or more.	A slight impact on the national Q-catch income, with a decrease that D It is possible was compensated for in time by He sees in the reduction in the GDP. and rate Labor, financial prices, or For markets purchasing power are only Yes; what negatively reflected on the One sector.	

Main impact category	national interest
Sub-category of impact	National infrastructure
Considerations	Does access to information disrupt vital national infrastructure (such as energy and telecommunications)? In the event of cyber attacks, will essential services in the Kingdom remain operational? Say, Is it available?

Impact level			
Top Secret	secret	restricted	Aor
High	middle	low	no here is a trace
The security and operations of vital national infrastructure are disrupted, many sectors are affected, and normal life is disrupted.	A short-term disruption or interruption in the security and operations of vital national infrastructure, with one or more sectors being affected.	Short-term damage or impact on the security and operations of local/ regional infrastructure.	

Main impact category	national interest
Sub-category of impact	Duties of government agencies
Considerations	Will disclosing information limit the ability of government agencies to carry out their daily operations and tasks? D

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
The inability of all government agencies to perform their main tasks and operations for a long period.	The inability of one or more government agencies to perform one or more of their main tasks for a short period.	The inability of one or more government agencies to perform one or more non-core tasks for a short period.	

Main impact category	Activities of the authorities
Sub-category of impact	Private sector profits
Considerations	Would disclosing the information lead to financial losses or bankruptcy for private entities that provide public services? For example, the possibility of fraud, illegal transfers of funds, and illegal seizure of assets? House Issued

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
A significant negative impact on private entities to the extent that it causes harm to vital national interests.	The entity incurs huge financial losses, which may lead to bankruptcy.	Limited damage is a limited financial loss to the entity or any of its assets.	There is no impact on the activities of the entities.

Main impact category	Activities of the authorities
Sub-category of impact	Tasks of private entities
Considerations	Will the disclosure of information cause harm to private entities managing public facilities? Will it result in the loss of their leading role or the loss of any of their assets? Will it lead to the termination of contracts for a large number of clients? Will it affect the private entity's competitiveness? You are doing To one side or Two guests?

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
A significant negative impact on private entities to the extent that it causes harm to vital national interests.	The inability of the entity to carry out its main tasks and the loss of the ability to compete to a large extent Mn -a, -i YR.	The inability of the group to perform one of its main tasks according to its competitive ability in a specific manner. Huh? MHa On Worm	There is no impact on the activities of the entities.

Main impact category	individuals
Sub-category of impact	Health/Safety of Individuals
Considerations	Will disclosing the information reveal the names or locations of persons, for example, the names and locations of confidential agents, persons subject to protection regulations? K? (on especially)

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
General or catastrophic loss of life, loss of life of an individual or group of individuals.	Serious harm or injury that threatens the life of an individual.	A minor injury without any threat to the life or health of the individual.	No effect on individuals

Main impact category	individuals
Sub-category of impact	Privacy
Considerations	Will disclosing information violate individuals' privacy?

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
Disclosure of personal data of an important person.	Data Disclosure Character for an important character And	Data Disclosure character of the individual.	No effect on individuals

Main impact category	individuals
Considerations	Will this infringe any intellectual property rights?

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
Affecting the national interest.			

Main impact category	the environment
Sub-category of impact	environmental resources
Considerations	Will this information be used to develop a service or product that could lead to environmental or natural destruction of the Kingdom? Resources

Impact level			
Top Secret	secret	restricted	general
High	middle	low	No trace
Irreversible catastrophic impact on the environment or natural resources.	long-term impact on the environment or natural resources .	Short-term or limited impact on the friendship environment or natural resources He is ignorant.	No impact on the environment.

Table 2: Impact assessment categories and scores according to data classification levels

4.1.4.Data classification controls

Based on the classification levels, entities determine and implement appropriate security controls to protect data to ensure that it is handled, processed, shared, and disposed of securely. If data is not classified upon creation or receipt in accordance with the classification criteria, it is treated as "restricted" until it is properly classified.

Data that has not been classified at the time of issuance of this policy must be classified within a specific period of time in accordance with an action plan prepared by the entity and approved by the entity's senior official.

Below are some examples of controls that can be used when classifying data. You can refer to the controls and guidelines issued by the National Cybersecurity Authority regarding data protection:

Protection marks

Text protection marks are applied to paper and electronic documents (including email messages) according to each classification level.

Access

Logical and physical access to data is granted based on the principles of "minimum privilege" and "need to know."

The right to access data must be denied once the professional service of employees with the entity has ended or been terminated.

Usage

Classified data is used according to the requirements of the classification levels. For example, the use of data classified as "Top Secret" is restricted to specific locations, whether physical – such as offices

- Or virtual using hardware encryption or special applications.

Storage

Data classified as "Top Secret," "Confidential," or "Restricted," as well as mobile devices that process or store such data, should not be left unattended.

Data classified as "Top Secret," "Confidential," and "Restricted" must be protected while stored unattended, whether physically or electronically, using one of the encryption methods approved by the National Cybersecurity Authority.

Data sharing

Entities identify appropriate physical and digital means for secure data exchange to ensure potential risks are minimized and data sharing regulations are complied with.

The mechanism for data exchange must be agreed upon, whether the entities will use the means currently used for data exchange or not, for example, the government integration channel, the national information center network, the secure government network, or set up a new direct connection, removable storage media, a wireless network, remote access, a virtual private network, etc.

Data retention

A schedule is prepared that specifies the retention period for all data.

The retention period is determined based on relevant commercial, contractual, regulatory and legal requirements.

The retention period schedule is reviewed periodically - annually or if changes occur in the relevant requirements.

Data disposal

All data is disposed of securely in accordance with the data retention schedule after obtaining approval from the Business Data Representative.

Data classified as “Top Secret” and “Confidential” that is controlled electronically is destroyed using the latest electronic media destruction methods.

All paper documents are disposed of using a paper shredder. A detailed record is kept of all data disposed of.

Archiving

Data is archived in secure storage locations according to the method recommended by the Business Data Representative.

Backups of archived data are kept.

Archived data classified as "Top Secret" and "Confidential" is protected using one of the encryption methods approved by the National Cybersecurity Authority. A detailed list of users authorized to access archived data is prepared and documented.

Declassification

Data shall be declassified or downgraded to an appropriate level after the expiration of the classification period when protection is not required or is no longer required at the original level of classification.

If data is incorrectly classified, the data user must notify the business data representative to determine the need for appropriate reclassification.

Factors that help in declassifying data must be identified when determining classification levels for the first time, and they must be recorded in the data assets register. These factors may include the following:

o A specific period of time after the data is created or received (for example: two years after creation)

o A specific period of time after the last action was taken on the data (for example: six months from the date of last use).

o After certain circumstances or events have a direct impact on the data (for example: a change in strategic priorities or a change in government agency personnel) o After a specific date has passed (for example, it is scheduled to be reviewed on January 1, 2021) o

Declassification - declassification - or downgrading of classification levels, apart from the obvious declassification facilitators, requires a sound understanding of the content of the classified data and the context in which it was received.

4.1.5. Steps to classify data

Step 1 - Specify all entity data

The first step for organizations is to inventory and identify all the data the organization has.

Step 2 - Assign a data classification officer

Once all data has been identified, the entity must delegate a person to take responsibility for the classification process. This is often the business data representative – a member of the entity's office – who understands the nature and value of the data within the entity. This person is the person who must bear responsibility for conducting the initial classification. Since there is more than one data officer within the entity, there may be more than one person responsible for classifying the data.

Step 3 - Conduct an impact assessment

The business data representative must follow the necessary steps to assess the potential impact of:

Disclosure of or unauthorized access to this data,

modification of or destruction of this data, or both,

failure to access this data in a timely manner

The impact assessment process begins with the application of the principle of "data origin availability" (in the development field) unless its nature or sensitivity requires higher levels of classification and protection; and of "data confidentiality" (in the political and security field) unless its nature or sensitivity requires lower levels of classification.

Step 3a - Determine the impact category:

The first element of the impact assessment process is to identify the main and sub-categories of the potential impact in any of the following main categories:

national interest

Activities of the authorities

Health or safety of individuals and

environmental resources

Step 3b - Determine the impact level:

The second element indicates that the business data representative must determine a specific level for each potential impact. The determination of the level depends on the following:

Duration of impact and difficulty of controlling damage.

Period of recovery and repair of damage after it occurs.

Impact size at the national, regional, multi-regional, single-region, multi-individual level...etc. **These criteria define the four levels of impact:**

High: Accessing or disclosing the data could cause serious or extremely serious harm. In the long run, it cannot be remedied or repaired.

Average: Accessing or disclosing data could cause serious or life-threatening harm. It is difficult to control.

Low: Accessing or disclosing the data will result in limited, controllable harm. Or intermittent, short-term damage that can be controlled.

No effect: Access to or disclosure of data does not result in any long-term harm or Short

All potential harms identified during the impact assessment process should be specific and evidence-based, in an attempt to limit the subjective judgment of the data collector.

The business data representative determines the data classification level based on the identified impacts and their levels:

High: The data is classified as “top secret.”

middle: The data is classified as “confidential”.

low: Further assessment is required (please see step4 and 5). **No**

trace: Data is classified as data.**"General"**.

A detailed description of the main considerations for each impact category and its level is found in Table (2). **“Categories and levels of data classification impact assessment.”**

Steps 4 and 5 should be considered when the specific impact level is low.

Step 6 is taken when data is classified as “top secret,” “confidential,” or “public.”

Step 4 – Identify relevant systems (only if the impact level is low).

Additional assessments should be made if the identified impact level is “low” in order to maximize the classification of data classified as “general”.

In this regard, the business data representative must study whether disclosing this data conflicts with the regulations of the Kingdom of Saudi Arabia, such as the Anti-Cybercrime Law and the E-Commerce Law... etc. If disclosing the data violates the regulations, then the data must be classified as “restricted” data. Otherwise, the business data representative must continue implementing step 5.

Step 5 - Balance the benefits of data disclosure and the negative impacts (only if the answer to Step 4 is “No”).

After ensuring the low level of impact and ensuring that disclosure will not be a violation of any applicable regulation, the potential benefits of disclosing such data must also be evaluated and whether these benefits outweigh the negative impacts. Potential benefits include using the data to develop new value-added services, increasing the transparency of government operations, or increasing individual engagement with the government.

If the benefits outweigh the negative effects, the data is classified as**"General"**If the benefits are less than the negative effects, the data is classified as**"Restricted"**.

Step 6 - Review the classification level

The data classification reviewer – a member of the entity’s office – must examine all classified data to ensure that the classification level determined by the business data representative is the most appropriate, and it is reviewed within one month of the initial classification.

Step 7 - Apply appropriate controls

The final step in the data classification process is to protect all data according to the classification level by applying relevant controls (see “Data Classification Controls”).

The classification process is completed when all data owned by the entity has been classified, classification levels have been verified, and relevant controls have been applied.

Once data is properly classified, entities can share it with other entities, or make it available and publish it as open data when classified as “public” data.

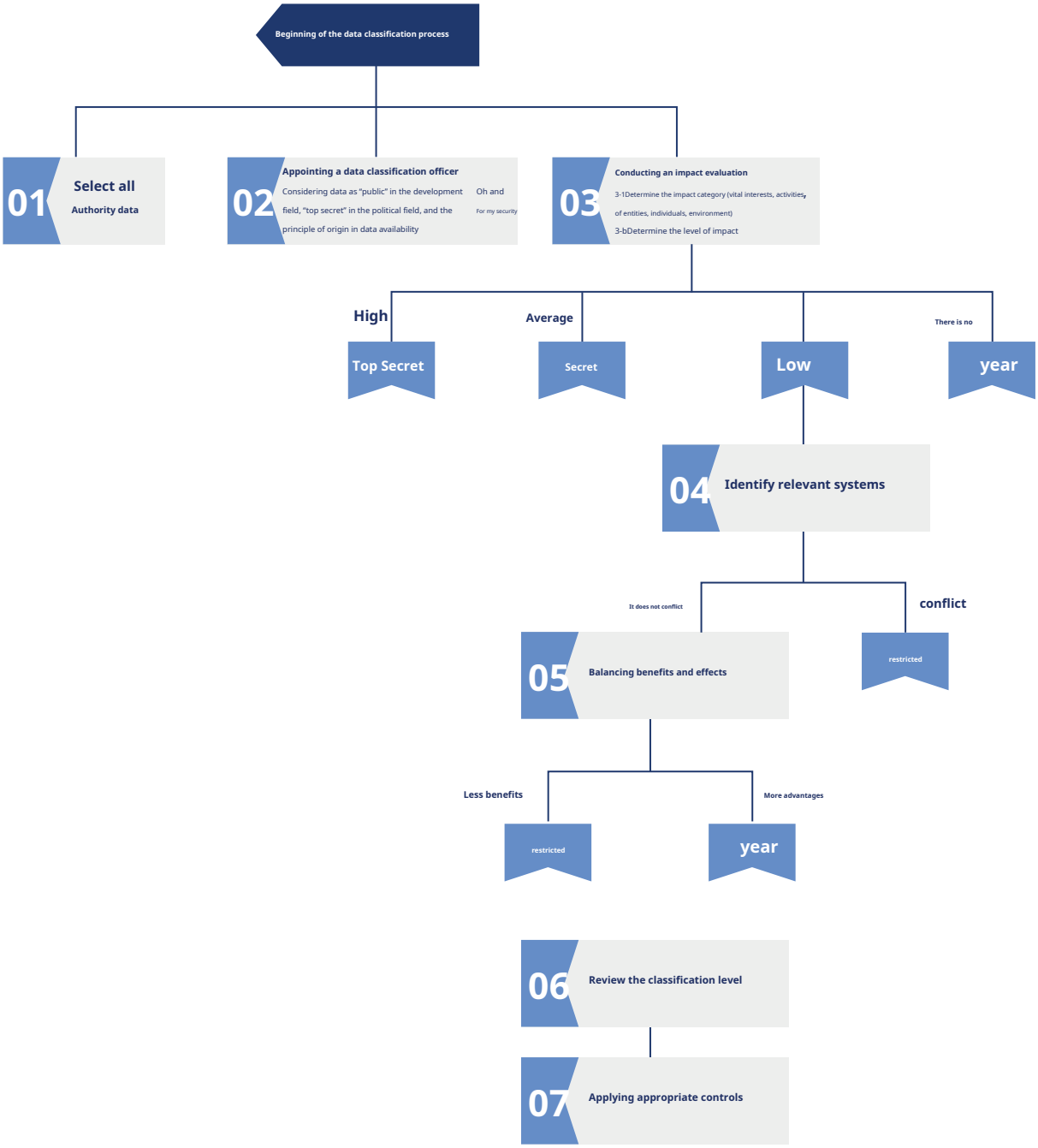


Figure (2) shows the steps required to perform data classification.

4.1.6. Roles and responsibilities within the entity

All entities shall assign persons responsible for performing the obligations assigned to each functional role related to the data classification process and the conditions for its protection, as stipulated below.

Business Data Representative: The person responsible for the data collected or retained by the entity, usually Be at a high management level, and be a business data representative responsible for:

Data classification: Classification of data collected by the entity or its affiliates.

Data collection: Ensure that data collected from multiple sources is classified at the highest levels. The classification used to classify any data individually.

Data classification coordination: Ensure that data exchanged between departments or entities is classified. And consistently protected.

Compliance with data classification (in coordination with business data specialists): Ensure that the data Protected according to specified controls.

Data classification references: The person responsible for reviewing and approving the data classification levels that Determined by the business data representative, usually a senior management level.

Business Data Specialist: Business data specialists are usually members of IT departments or Information security, or both, and is responsible for protecting data by implementing the approved controls specified in the "Data Classification Controls" section. In addition, maintaining and supporting the systems, databases, and servers that store data. The responsibilities of the business data specialist include: **Access Control:**Ensure that access control controls are implemented, monitored and reviewed in accordance with For data classification levels determined by the business data representative.

Review reports: Sending an annual report to data officers on the availability of classified data. Its safety and confidentiality.

Data backup: Perform regular data backups. **Data validation:**Check data periodically. **Data recovery:** Recover data from backup media.

Monitoring activity: Monitoring and recording activities involving data, including data Relating to the person who accesses this data.

Data classification compliance (in conjunction with data custodians): Ensure data classification The entity and its protection after the process described in this policy and in accordance with the specified controls.

Data user: The employee who handles, accesses, uses, or updates the data. For the purpose of performing a task authorized by the business data representative, users shall utilize the data in a manner consistent with the specified purpose, as well as comply with this policy and all policies related to the use of data in the Kingdom of Saudi Arabia. The first official in the entity shall assign whomever he deems competent to perform these roles.

Data Protection Policy

Character

4.2. Personal Data Protection Policy

4.2.1. Scope

The provisions of this policy apply to all entities in the Kingdom that process personal data, in whole or in part, as well as to external entities that process personal data relating to individuals residing in the Kingdom, which is done via the Internet or any other means.

The scope of application of this policy excludes the collection of personal data from someone other than its owner directly - without his knowledge - or processing it for a purpose other than that for which it was collected, or disclosing it without his consent, or transferring it outside the Kingdom in the following cases:

1. If the controlling authority is a government entity and the collection or processing of personal data is required to achieve Regulatory requirements in accordance with the laws, regulations and policies in force in the Kingdom, or to meet judicial requirements or to implement 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 Vital interests of individuals.

4.2.2. Main principles of personal data protection

The first principle: responsibility

The privacy policies and procedures of the controlling entity shall be defined, documented, and approved by the entity's senior official (or his/her delegate), and published to all parties concerned with their implementation.

The second principle: transparency

A notice of the controller's privacy policies and procedures must be prepared, specifying the purposes for which personal data are processed in a specific, clear and explicit manner.

Principle 3: Choice and Consent

All possible options for the personal data owner must be identified and his consent (implicit or explicit) must be obtained regarding the collection, use or disclosure of his data.

Principle 4: Limiting Data Collection

The collection of personal data shall be limited to the minimum amount of data that enables the purposes specified in the privacy notice to be achieved.

Principle 5: Limiting Data Use, Retention, and Disposal

The processing of personal data shall be restricted to the purposes specified in the privacy notice, for which the data subject has given his implicit or explicit consent, and shall be retained for as long as necessary to achieve the specified purposes or as required by the applicable laws, regulations and policies in the Kingdom, and shall be destroyed in a secure manner that prevents leakage, loss, embezzlement, misuse or unauthorized access.

Principle 6: Access to Data

The means by which the data owner can access his personal data to review, update, and correct it must be identified and provided.

Principle 7: Limiting Data Disclosure

Disclosure of personal data to external parties shall be restricted to the purposes specified in the privacy notice and for which the data subject has provided implicit or explicit consent.

Principle 8: Data Security

Personal data shall be protected from leakage, damage, loss, misappropriation, misuse, modification, or unauthorized access – in accordance with the provisions of the National Cybersecurity Authority and the relevant authorities.

Principle 9: Data Quality

That personal data is kept accurately, completely, and directly relevant to the purposes specified in the Privacy Notice.

Principle 10: Monitoring and Compliance

To monitor compliance with the controller's privacy policies and procedures, and to handle privacy-related inquiries, complaints and disputes.

4.2.3. Data Subject Rights

Firstly: The right to information, including being informed of the legal basis or actual need to collect his data. The character, the purpose of it, and not His data is later processed in a manner that is inconsistent with the purpose for which it was collected. For which he gave his implicit or explicit consent.

Second: The right to withdraw his consent to the processing of his personal data - at any time - unless it is There are legitimate purposes that require the opposite.

Third: The right to access his personal data held by the controlling authority, in order to review it and request Correcting, completing, or updating it, requesting the destruction of any of it that is no longer needed, and obtaining a copy of it in a clear format.

4.2.4. Obligations of the Controller

1.The controlling authority shall be responsible for preparing and implementing policies and procedures related to data protection. The person in charge of the entity - or his delegate - shall be responsible for approving and adopting it.

2.The controlling authority shall establish a data governance unit that is (linked to the data management offices in the authorities Government entities established pursuant to Royal Decree No. 59766 dated 11/20/1439 AH) or independent (in private sector entities) and entrusted with the responsibility of developing, documenting and monitoring the implementation of policies and procedures approved by the entity's senior management, provided that the unit's tasks and responsibilities include setting appropriate standards to determine the levels of sensitivity of personal data.

3.The controller shall assess the risks and potential impacts of personal data processing activities and display The evaluation results are submitted to the entity's senior official – or his/her delegate – to determine the level of risk acceptance and approval.

4.The controlling authority shall review and update contracts, service level agreements and operating agreements in accordance with With the privacy policies and procedures approved by the entity's senior management.

5.The controlling authority shall prepare and document the necessary procedures to manage and address privacy violations. Determine the tasks and responsibilities related to the competent work team, and the cases in which the regulatory body and the office are notified according to the administrative hierarchy - based on measuring the severity of the impact.

6.The controlling authority shall prepare awareness programmes to enhance the culture of privacy and raise the level of awareness in accordance with For privacy policies and procedures approved by the entity's senior management.

7.The data owner shall be notified - in an appropriate manner and at the time of data collection - of the purpose and legal basis.

The actual need, means and methods used to collect, process and share personal data, as well as security measures to ensure privacy protection in accordance with the applicable laws, regulations and policies in the Kingdom.

8.The data owner must be notified of other sources used in the event that data is collected. Additional indirectly (from other parties).

9.The data subject shall be provided with the available options regarding the processing of personal and automated data.

Preferences used to exercise these options are (-out Preferences, Opt-in and Opt).

10.The data subject's consent must be obtained to process personal data after specifying the type of consent.

(Explicit or implicit) depending on the nature of the data and the methods of collecting it.

11.The purpose of collecting data must be consistent with the applicable regulations, rules and policies.

The Kingdom and has a direct relationship with the entity's activity.

12.The data content should be limited to the minimum data necessary to achieve the purpose of

Collect it.

13.Data collection shall be restricted to the pre-prepared content (shown in the rule).12) It is done in a way

Fair (direct, clear, safe, and free from deception or misleading methods).

14.The use of data shall be limited to the purpose for which it was collected.

15.The controlling authority shall prepare and document the data retention policy and procedures in accordance with the specified purposes.

And the relevant regulations and legislation.

16.The controlling authority shall store and process personal data within the geographical borders of the Kingdom to ensure that:

Maintaining the national digital sovereignty of this data, it may not be processed outside the Kingdom except after the controlling authority obtains written approval from the regulatory authority, after coordination between the regulatory authority and the office.

17.The controlling authority shall prepare and document a data disposal policy and procedures for data destruction.

In a secure manner that prevents its loss, misuse, or unauthorized access - including operational, archived, and backup data - in accordance with what is issued by the National Cybersecurity Authority.

18. The controlling authority shall include provisions for data retention and disposal policies in contracts.

If these tasks are assigned to other processing entities.

19. The controlling authority shall determine and provide the means by which the data owner can access

To his personal data to review and update it.

20. The controlling authority must verify the identity of individuals before granting them access to their personal data.

In accordance with the controls approved by the National Cyber Security Authority and the relevant authorities.

21. It is prohibited to share personal data with other parties except in accordance with the specified purposes and after the owner's approval.

Data in accordance with regulations, rules and policies, provided that other parties are provided with the privacy policies and procedures in place and included in contracts and agreements.

22. Data owners should be notified and their consent should be obtained if data is shared with other parties. For use for purposes other than those specified.

23. The controlling authority shall obtain the office's approval - after coordination with the regulatory authority - before participation.

Personal data with other parties outside the Kingdom.

24. The controlling authority shall prepare, document and implement the necessary procedures to ensure the accuracy of personal data. Its completeness, modernity and relevance to the purpose for which it was collected.

25. That the administrative controls and technical measures approved in the entity's information security policies be used. To ensure the protection of personal data, including, but not limited to:

Granting data access permissions according to employees' tasks and responsibilities in a manner that prevents overlap of jurisdiction and avoids the dispersion of responsibilities.

Implementing administrative procedures and technical measures that document the stages of data processing and provide the ability to identify the user responsible for each of these stages (usage logs).

Employees who handle data processing operations must sign a pledge to maintain the data and not disclose it except in accordance with policies, procedures, regulations, and legislation.

Selecting employees who handle data processing operations who are characterized by honesty and responsibility, in accordance with the nature and sensitivity of the data and the access policy approved by the entity.

Use appropriate security measures - such as encryption, and isolating the development and testing environment from the operating environment - to secure and protect personal data in a manner commensurate with its nature, sensitivity, and the media used to transfer and store it, in accordance with what is issued by the National Cyber Security Authority and the relevant authorities.

26. The controlling authority shall be responsible for periodically monitoring compliance with privacy policies and procedures. It is presented to the entity's senior official - or his/her authorized representative - and the corrective actions to be taken in the event of non-compliance are identified and documented, and the regulatory body and the office are notified according to the organizational hierarchy.

4.2.5. General Provisions

Firstly: Regulatory authorities shall align the provisions of this policy with their regulatory documents and disseminate it to All its affiliated or related entities, in order to achieve integration and ensure the achievement of the desired goal of preparing this policy.

secondly Regulators monitor compliance with this policy periodically.

Third: Controlling entities must comply with this policy and document compliance in accordance with the mechanisms and procedures that Determined by regulatory authorities.

Fourth: Control authorities must inform the regulatory authorities immediately and without delay and no later than72 hours from the occurrence or discovery of any personal data leak, in accordance with the mechanisms and procedures determined by the regulatory authorities.

Fifth: When contracting with processing entities, the controlling authorities must periodically verify compliance with The processing entities shall implement this policy in accordance with the mechanisms and procedures determined by the regulatory authorities, including any subsequent contracts concluded by the processing entities.

Sixth: The Office exercises the roles and duties of regulatory bodies over control bodies not subject to regulatory bodies. Organizational.

Seventh: Regulators may establish additional rules for processing specific types of personal data. According to the nature and sensitivity of this data, after coordination with the office.

Eighth: The regulatory authorities, after coordination with the office, prepare the mechanisms and procedures that regulate The process of handling complaints according to a specific time frame and according to the organizational hierarchy of the authorities.

Ninth: The office sets the necessary standards that help the controlling authorities to know whether the appointment of Data Protection Officer is a basic or optional requirement.

Data Sharing Policy

4.3. Data Sharing Policy

4.3.1. Scope

The provisions of this policy apply to all government agencies to share data produced by these agencies - with other government agencies, private entities, or individuals - regardless of the source, form, or nature of this data. This includes paper records, e-mail messages, data stored on electronic media, audio or video tapes, maps, photographs, manuscripts, handwritten documents, or any other form of recorded data.

The provisions of this policy do not apply to the sharing of private sector data or data held by individuals. The provisions of this policy also do not apply if the party requesting the data is a government entity and the request is for security purposes or to meet judicial requirements.

4.3.2. Key principles of data sharing

The first principle: promoting a culture of participation

All government agencies are required to share the primary data they produce to achieve integration among these agencies and adopt the "one-time principle" to obtain data from its correct sources and limit duplication, conflict, and multiple sources. In the event that data is requested from a source other than its primary source, the agency required to share this data must obtain the approval of the primary agency - the source of the data.

- Before sharing it with the requesting party.

The second principle: legitimacy of the purpose

Data shall be shared for legitimate purposes based on a regulatory basis or justified practical need aimed at achieving a public interest without causing any harm to national interests, the activities of entities, the privacy of individuals, or the safety of the environment - with the exception of data and entities exempted by royal orders.

Principle 3: Authorized Access

All parties involved in data sharing must have the authority to access, obtain, and use this data (which may require security scanning depending on the nature and sensitivity of the data), in addition to the knowledge, skills, and properly qualified and trained persons to handle the shared data.

The fourth principle: transparency

All parties involved in data sharing operations must provide all information necessary for data exchange, including: the data required, the purpose of its collection, the means of its transmission, the methods of its preservation, the controls used to protect it, and the mechanism for its disposal.

Principle 5: Shared Responsibility

All parties involved in data sharing shall be jointly responsible for data sharing and processing decisions in accordance with the specified purposes, and ensure the implementation of the security controls stipulated in the data sharing agreement, and relevant regulations, legislation and policies.

Principle 6: Data Security

All parties involved in data sharing must implement appropriate security controls to protect data and share it in a safe and reliable environment in accordance with relevant regulations and legislation, and in accordance with what is issued by the National Cybersecurity Authority.

Principle 7: Ethical Use

All parties involved in data sharing must apply ethical practices during the data sharing process to ensure that data is used within a framework of fairness, integrity, honesty, and respect, and not be satisfied with adhering to information security policies or adhering to relevant regulatory and legislative requirements.

4.3.3. Steps required to perform the data sharing process

The basic steps for the data sharing process have been identified to help entities standardize sharing practices and ensure that all necessary controls and requirements are met—which may not exceed three months. Figure 3 below illustrates the steps required for data sharing.

1.The applicant - whether a government or private entity or an individual - sends a data sharing request. To the office of the entity required to share data, provided that the request is sent via the entity's office if the requester is a government entity.

2.The office of the entity requested to share data will refer the request to the business data representative. The specialist, in turn, directs this request to a business data specialist to evaluate and process it.

3.The business data specialist checks the classification level of the required data:

A.In the event that the classification level is not specified, the office of the entity required to participate must: Data – Classify the required data according to the data classification policy.

for. If the classification level is set to "General", the business data specialist can share The requested data is not evaluated in accordance with the main principles of data sharing.

T.In the event that the classification level is determined as "Restricted", "Confidential" or "Highly Confidential", the Business Data Specialist Evaluate the application according to the main principles of data sharing.

4.The business data specialist in the office of the entity required to share data must complete: The sharing process is complete if all data sharing principles are fully met.

5.The business data specialist in the office of the entity required to share the data may not continue to Data sharing in the event that one or more of the data sharing principles are not met. The business data specialist in the entity's office must return the request to the applicant with comments and provide an opportunity to meet all non-compliant data sharing principles.

6.When all data sharing principles are met, the business data specialist obtains approval. Business data representative to complete the data sharing process.

7.The business data specialist in the office of the entity required to share the data determines the controls. Appropriate to ensure compliance with the principles of data sharing and achieving the objectives specified for each. An agreement must also be reached between the business data specialist in the entity's office, the applicant, and other parties participating in the sharing process to implement these controls.

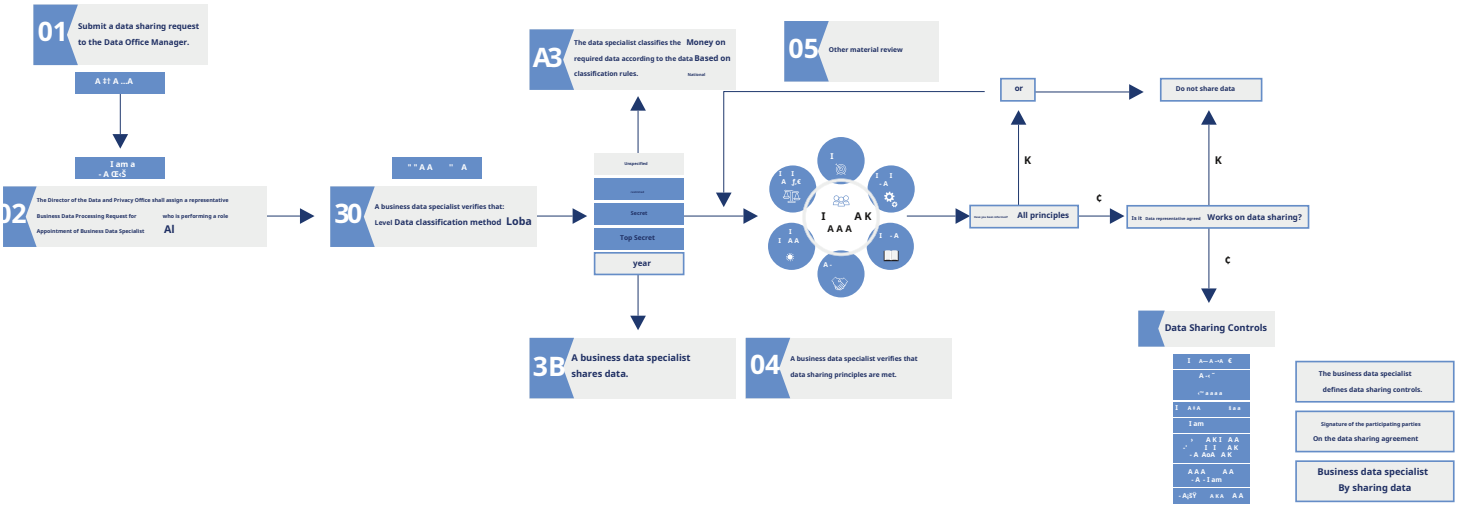
8.After agreeing on the data sharing controls and committing to implementing them, the business data specialist should:

It is explained in detail in the agreement and all parties participating in the participation process must

Signing a data sharing agreement.

9.The office of the entity may share the required data with the requesting entity after signing a sharing agreement.

Data.



4.3.4. Timeframe for the data sharing process

The government agency required to share data shall evaluate the request within a period not exceeding (30) days from the date of receipt of the request, and notify the applicant of the decision to participate, provided that the decision is written and reasoned (steps 2 to 4 of the data sharing process explained above).

In the event that the participation request is not approved, the applicant has the right to complete the requirements to meet all principles and request an appeal from the business data specialist to re-evaluate the request and issue the participation decision within a period of time not exceeding (14) days from the date of receipt (Step 5 of the data sharing process).

After obtaining the Business Data Representative's approval to continue the sharing process (Step 6 of the Data Sharing Process), the Business Data Specialist shall develop and implement appropriate controls for data sharing and prepare a data sharing agreement within a period of time not exceeding (60) days from the date of the Business Data Representative's approval (Step 7 of the Data Sharing Process).

After signing the data sharing agreement (Step 8 of the data sharing process), the business data specialist shares the data with the applicant within (7) days from the date of signing the agreement (Step 9 of the data sharing process).

4.3.5. Data Sharing Controls

All parties involved in the data sharing process must agree to the necessary controls to appropriately manage and protect the shared data:

Systematic basis:

(Related principles: Principle 1: Promoting a culture of participation, Principle 2: Legitimacy of purpose, Principle 5: Shared responsibility, Principle 7: Ethical use)

The legal basis or actual need for data sharing must be clarified, including, for example, the entity's organization, a royal/royal decree authorizing the entity to share data, or signed agreements. Data classification standards must be adhered to, as well as intellectual property rights and personal data privacy.

Delegation:

(Related principles: Principle 3: Authorized access, Principle 6: Data security)

To identify the parties and persons authorized to request and receive data (compliance with the data classification policy - controls on use and access to data can be verified).

Data type:

(Related principles: Principle 1: Promoting a culture of participation, Principle 2: Legitimacy of purpose, Principle 4: Transparency)

Ensure that the required data is included in the main data produced by the entity to ensure that the data is requested from its correct source.

To specify the minimum amount of data required to achieve the specified purposes.

To specify the required data, its format, and the requirements for modifying or changing it (such as data format, data accuracy, level of detail, data structure, type of data (raw or processed data).

Data preprocessing:

(Related principles: Principle 6: Data security)

To determine whether there is a need to process the data before sharing it, and if necessary, to agree on the required processing methods - for example, blocking, anonymization, and aggregation (provided that the data is not processed in a way that changes the content).

To assess the quality, accuracy, and integrity of the required data and determine whether it requires improvement before sharing it. If necessary, the entity's office must audit the data before sharing it.

Data sharing methods:

(Related principles: Principle 6: Data security)

Compliance with data protection regulations issued by the National Cybersecurity Authority.

Determine the means of sharing physical and digital data.

The security and reliability of sharing methods must be verified to reduce potential risks.

Approved secure sharing methods can also be used between parties.

The data sharing mechanism must be determined, and whether the business data specialist will transfer the data directly to the applicant or a service provider will be used to complete the sharing process. It must be determined whether existing sharing media will be used (e.g., the Government Integration Channel, the National Information Center Network) or different media will be used (wireless Internet, remote access, virtual private network, application programming interface).

A mechanism for destroying the physical media used in data sharing must be agreed upon.

Data Use and Retention:

Related principles: Principle 2: Legitimacy of purpose, Principle 4: Transparency, Principle 6: Data security, Principle 7: Ethical use

To determine data protection requirements when sharing data, and to implement specific controls to protect data after sharing it.

To impose appropriate restrictions on the permitted use or processing of the data (if any), such as processing restrictions, spatial or temporal restrictions, or exclusive or commercial rights.

The rights of all parties involved in the process of participating in the audit and review process should be determined.

To agree on dispute settlement and arbitration procedures.

To determine whether there is a third party to benefit from the data after sharing it and agree on the mechanism regulating this.

Data sharing duration, number of sharing times, and unsharing:

(Related principles: Principle Two: Legitimacy of purpose, Principle Six: Data security)

Specify the duration of data sharing and the deadline for accessing or storing data.

Specify the number of times data will be shared, the requirements for review and amendments, and the actions to be taken upon termination of the agreement (such as anonymizing data holders, revoking access to data, or destroying data).

To identify the parties who have the right to terminate data sharing before the agreed date, the legal document, and the permitted notice period.

Liability provisions:

(Related principles: Principle 5: Shared responsibility)

It is agreed to determine responsibilities in the event of non-compliance with the terms of the agreement, and other obligations between the participating parties, such as termination of the agreement and corrective measures.

To determine the rules related to liability provisions when sharing incorrect data, the presence of technical problems during the data transfer process, or the unintentional or irregular loss of data, which may cause other damages.

4.3.6. General Data Sharing Rules

Here are some general rules that entities should follow when sharing data:

1. All parties must give priority to reliable and secure means of sharing data.

These include, for example, the Government Integration Channel and the National Information Center Network.

2. The business data specialist in the office of the entity required to participate is responsible for participating.

Data after fulfilling all data sharing principles, in addition to determining appropriate controls for sharing.

3. Each entity must appoint or delegate the appropriate person - according to the required qualifications and training.

- To deal with data in a correct manner, provided that he is authorized to request, receive, access, store and destroy shared data.

4. The identity of personal data subjects must be concealed, unless it is necessary for the purpose of participation.

The necessary controls to maintain the privacy of data subjects in accordance with the Personal Data Privacy Policy.

5. Metadata must be attached (When sharing data in cases where it is required (metadata).

6. The parties involved in data sharing are responsible for protecting and using the data in accordance with

For specific purposes, the entity's office has the right to review the extent of compliance periodically or randomly in accordance with the controls specified in the data sharing agreement.

7. The office is preparing a guideline for data sharing, which includes a data sharing request form.

Standard data sharing agreement template.

8. The regulatory authorities, after coordination with the office, prepare the mechanisms, procedures and controls.

Related to the settlement of the dispute according to a specific time frame.

9. In the event of a dispute between the parties involved in the data sharing process, the affiliated entities have the right to:

The same regulatory body shall notify the regulatory body and request a settlement of the dispute between the participating parties. If the dispute is not resolved, the office shall be notified of this, and the office shall undertake the settlement of the dispute if the two parties are not subject to the same regulatory body.

10. In the event that there is an aspect of data sharing that is not covered by this policy, the entity's office has the right to:

Establish additional rules that do not conflict with the principles of data sharing, providing sufficient justification and notifying the office thereof.

11. The parties involved in data sharing must find the appropriate balance between the need to share Data and ensuring the protection of data confidentiality and potential risks to the individual or society.

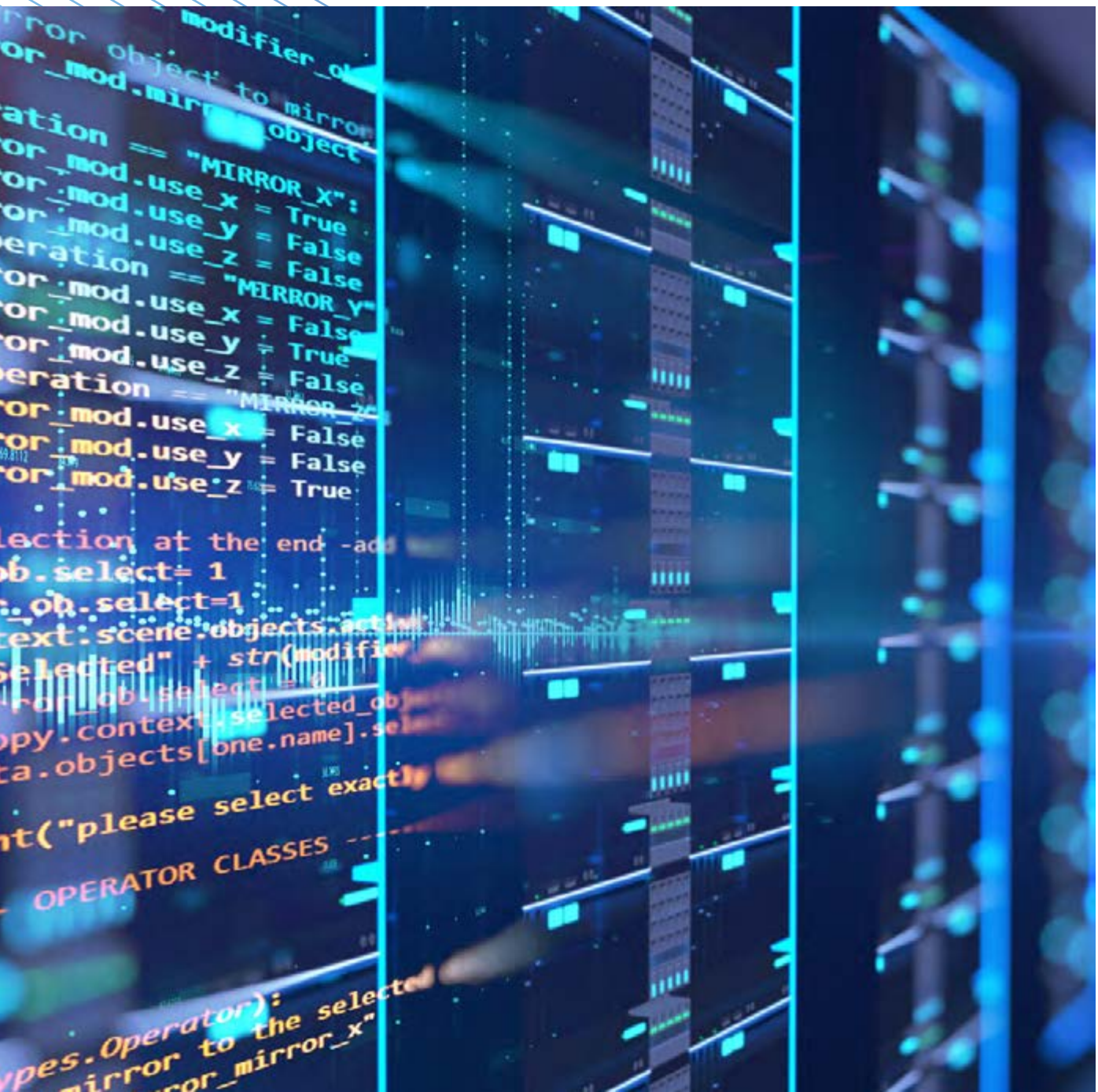
12. Entities must maintain records of data sharing requests and decisions related to them.

13. Entities shall develop, adopt and publish their data sharing policy in accordance with this Policy.

14. When entities receive shared data, they must not share it with another party or entity. Without the consent of the data producer.

15. The entity shall be responsible for monitoring and implementing this policy.

Freedom of Information Policy



4.4. Freedom of Information Policy

4.4.1. Scope

This policy applies to all individual requests to view or obtain public information – unprotected – produced by public bodies, regardless of its source, form or nature – including paper records, emails, information stored on computers, audio or video tapes, maps, photographs, manuscripts, handwritten documents, or any other form of recorded information.

The provisions of this policy do not apply to protected information:

1.Information the disclosure of which would harm the national security of the state, its policies or interests, or Her rights.

2.Military and security information.

3.Information and documents obtained under an agreement with another country and classified as Protected.

4.Investigations, inquiries, seizures, inspections and monitoring operations related to a crime or violation or to threaten.

5.Information that includes recommendations, suggestions or consultations for the purpose of issuing legislation or a decision Governmental not yet issued.

6.Information of a commercial, industrial, financial or economic nature, the disclosure of which would result in: To achieve a profit or avoid a loss in an illegal manner.

7.Scientific or technical research, or rights that include intellectual property rights that lead to Disclosing it would violate a moral right.

8.Information related to competitions, bids and tenders, the disclosure of which would lead to a breach Fair competition.

9.Information that is confidential or personal under another system, or requires certain regulatory procedures To access or obtain it.

4.4.2. Main principles of freedom of information

The first principle: transparency

The individual has the right to know information related to the activities of public bodies in order to enhance the system of integrity, transparency and accountability.

The second principle: necessity and proportionality

Any restrictions on the request to view or obtain protected information received, produced or handled by public bodies must be clearly and explicitly justified.

The third principle: The basis of public information is disclosure.

Every individual has the right to access public, non-protected information. The applicant does not necessarily have to have a certain status or interest in this information to be able to obtain it, nor is he subject to any legal accountability related to this right.

The fourth principle: equality

All requests for access to or access to public information are handled on the basis of equality and non-discrimination between individuals.

4.4.3. Individuals' rights to access or obtain public information

Firstly: The right to access and obtain any unprotected information held by any public authority. **secondly:**The right to know the reason for the refusal to view or obtain the requested information. **Third:**The right to appeal a decision to reject a request to view and obtain the required information.

4.4.4. Obligations of public entities

1. The public authority shall be responsible for preparing and implementing policies and procedures related to the exercise of the right to Access to or obtaining public information, and the official in charge of the entity shall be responsible for approving and adopting it.
2. The public authority shall establish an administrative unit that is linked to the data management offices in the authorities. The government unit, which was established pursuant to Royal Decree No. 59766 dated 11/20/1439 AH, is entrusted with the responsibility of developing, documenting, and monitoring the implementation of policies and procedures approved by the entity's senior management related to the right of access to information. The unit's tasks and responsibilities shall include setting appropriate standards to determine data classification levels in the event of their non-existence – in accordance with the data classification policy – and using them as a primary reference when processing requests for access to information. Public or obtain it.

3. The public authority shall determine and provide the possible means (general information request forms) - whether Whether paper or electronic forms – through which an individual can request access to or obtain public information.

4. The public authority shall verify the identity of individuals before granting them the right to access public information. Or obtain it in accordance with the controls approved by the National Cyber Security Authority and relevant authorities.

5. The authority shall establish the necessary standards to determine the fees charged for processing information requests. Access to or obtaining public information is based on the nature and volume of the data, the effort expended, and the time taken - in accordance with the data monetization policy document. The public entity shall document all records of requests to access or obtain information and the decisions taken regarding the requests. These records shall be reviewed to address cases of misuse or non-response.

6. The public authority shall prepare and document policies and procedures for maintaining and disposing of records of requests. In accordance with the regulations and legislation related to the work and activities of the entity.

7. The public authority shall prepare and document the necessary procedures for managing, processing and documenting extension requests. Rejected requests, determining the tasks and responsibilities of the relevant work team, and the cases in which the regulatory body and the office are notified according to the administrative hierarchy, in accordance with the time period specified for processing requests.

8. The public authority shall notify the individual - in an appropriate manner - if the application is rejected in whole or in part. With clarification of the reasons for rejection, the right to appeal, and how to exercise this right within a period not exceeding (15) days from the decision being taken.

9. The public authority shall prepare awareness programmes to enhance the culture of transparency and raise the level of awareness in accordance with Freedom of information policies and procedures approved by the entity's senior management.

10. The public body should be responsible for monitoring compliance with freedom of information policies and procedures in a comprehensive manner. It is periodically presented to the first official in the entity or his delegate. The corrective measures that will be taken in the event of non-compliance are also determined and documented, and the regulatory body and the office are notified according to the administrative hierarchy.

4.4.5. Main steps for viewing or obtaining information

Key requirements for requests for access to or obtaining public information:

1.The application must be in writing or electronically.

2.The "General Information Request Form" approved by the public authority must be completed.

3.The request must be for the purpose of accessing or obtaining public information.

4.The application form must include details on how the final decision and notifications will be sent to the individual. (National address, e-mail, or website of the entity...etc.)

5.The application form must be sent directly to the public authority.

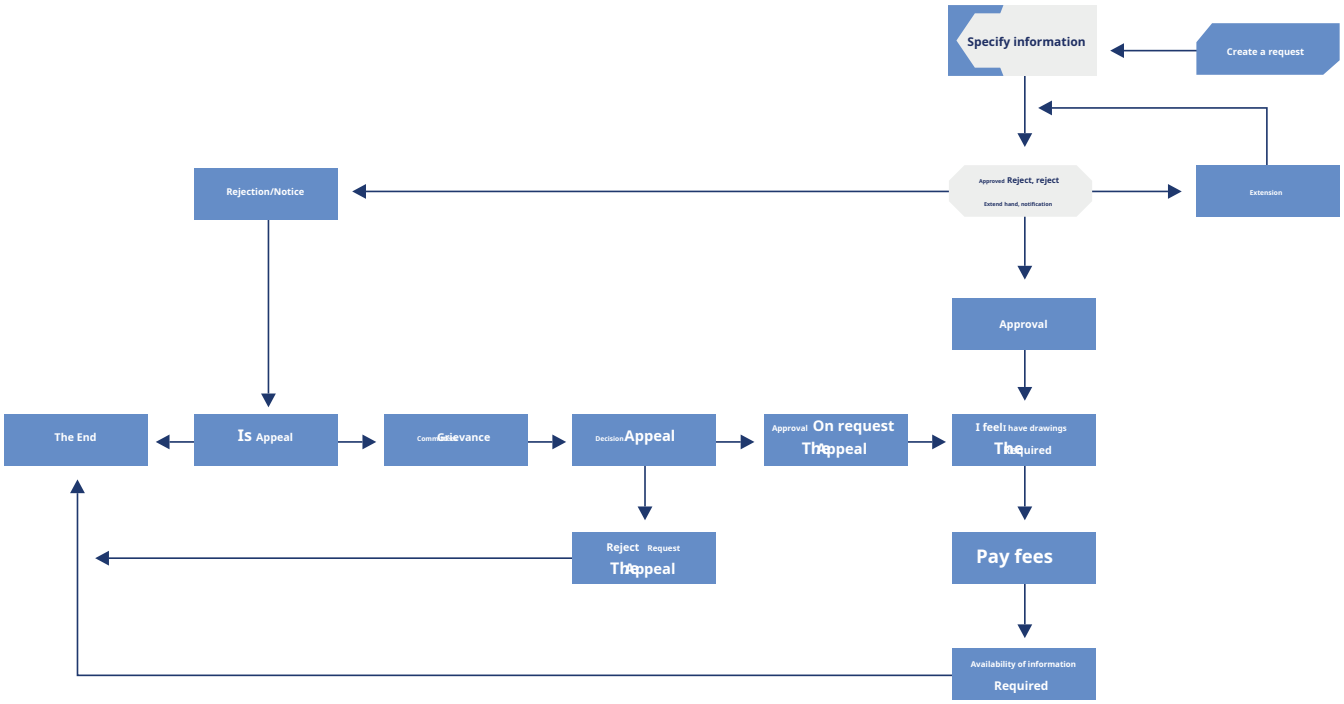


Figure 2 Main steps for requesting or obtaining public information

Main steps for requesting access to or obtaining general information:

Firstly: Applications are submitted by filling out the "General Information Request Form" – electronically or in paper form – And submit it to the public authority that has the information.

Second: The public authority shall, within a specific period of time ((30 days) upon receipt of a request to view or obtain public information, by taking one of the following decisions:

1. **Approval:**In the event that the public authority approves the request to access or obtain information In whole or in part, the individual must be notified in writing or electronically of the applicable fees, and the public entity must make this information available to the individual within a period of time not exceeding (10) business days from receiving the amount.
2. **Rejection:**In the event that the request for access to or obtaining information is rejected, it must be The refusal shall be submitted in writing or electronically, and shall include the following information:

   Specify whether the application was rejected in whole or in part.

   Reasons for rejection, if applicable.

   The right to appeal this refusal and how to exercise this right.
3. **Extension:**If the request for access to information cannot be processed in a timely manner, it should be The public authority may extend the period in which the response will be made for a reasonable period according to the size and nature of the information requested - for example, not exceeding (30) additional days - and provide the individual with the following information:

   Extension Notice and Date Expected to Complete Application

   Reasons for Delay

   The right to appeal this extension and how to exercise this right.
4. **Notice:**If the required information is available on the authority's website, or is not within its jurisdiction, The individual must be notified of this in writing or electronically, and the notification must include the following information:

   Type of notification, for example, whether the requested data is available on the entity's website or not within its jurisdiction.

   The right to appeal this notice and how to exercise this right.

Third: In the event that an individual wishes to appeal the rejection of the application by a public authority, he can submit a notification The grievance shall be submitted in writing or electronically to the office of the entity within a period not exceeding (10) working days from the date of receipt of the decision of the public entity. The grievance committee at the office of the entity shall review the request, take the appropriate decision, and notify the individual of the review fees - which shall be refunded in the event that the committee approves the request - and the appeal decision.

4.4.6. General Provisions

Firstly: Public authorities shall align this policy with their regulatory documents – policies and procedures – And circulate it to all its affiliated or related entities in a way that achieves integration and ensures the achievement of the desired goal of its preparation.

Second: Public authorities must balance the right to access information with the requirements. Other necessities such as achieving national security and maintaining the privacy of personal data. **Third:**Public entities must comply with this policy and document compliance periodically in accordance with the mechanisms. And the procedures determined by these bodies after coordination with the office.

Fourth: The regulatory authorities, after coordination with the Office, shall prepare the mechanisms, procedures, and controls related to handling complaints according to a specific timeframe and in accordance with the organizational hierarchy.

Fifth: Public authorities must notify the office in the event of a refusal to request access or obtain information. General information or extending the period specified for submitting this information, which is within the scope. **Sixth:**The public authority must, when contracting with other parties - such as companies that directly... Public Services - To periodically verify the compliance of other entities with this policy in accordance with the mechanisms and procedures determined by the entity, provided that this includes any subsequent contracts concluded by other entities. **Seventh:**Public authorities have the right to establish additional rules for processing requests related to specific types of General information according to its nature and sensitivity after coordination with the office.

Eighth: Public entities must prepare forms for viewing or obtaining public information - whether Whether paper or electronic, it specifies the necessary information and the possible means of providing the required information.

4.4.7. Freedom of information and open data

Open data programs and policies are usually prepared and developed around the world to support the growth of the national economic agenda and innovation. There is no doubt that making a specific set of public information available to researchers, entrepreneurs, innovators, and startups helps create a favorable environment for business growth and indicates the presence of an open and transparent government.

Open data programs and policies are a proactive step taken by authorities to preserve the right to access public information by making available or publishing a specific set of information – as open data – before access or obtaining it is requested. Therefore, effective open data programs and policies reduce the volume of requests for access to public information, which leads to a reduction in government expenditures related to processing requests.

Open Data Policy

4.5. Open Data Policy

Open data is a subset of public information according to the classification levels described in the Data Classification Policy.

4.5.1. Scope

The provisions of this policy apply to all public data and information - unprotected - produced by public entities, regardless of their source, form or nature - including paper records, emails, information stored on computers, audio or video tapes, maps, photographs, manuscripts, handwritten documents, or any other form of recorded information.

4.5.2. Key principles of open data

The first principle: the origin of data is availability.

This principle ensures that public entities' data is made available to all by disclosing it, enabling access to it, or using it unless its nature requires non-disclosure or the protection of its privacy or confidentiality. **Principle 2:**

Open format and machine readability

Data is made available in a machine-readable format that allows for automatic processing – and is saved in commonly used file formats such as CSV, XLS, JSON, or XML.

Principle 3: Data Freshness

The latest version of open data sets is published regularly and made publicly available as soon as it becomes available. Data collected by public entities is published as soon as possible after collection, and priority is given to data whose usefulness decreases over time.

The fourth principle: inclusiveness

Open datasets should be comprehensive and include as much detail as possible, and should reflect the recorded data in a manner that does not conflict with the personal data protection policy. Metadata that explains and interprets the raw data should also be included, along with explanations or equations that clarify how the data was extracted or calculated.

Principle 5: Non-discrimination

Datasets must be made available to everyone without discrimination and without the need for registration – anyone can access published open data at any time without the need to verify identity or provide justification for access.

Principle 6: Free of charge Open data should be made freely available to everyone.

Principle Seven: Open Data Licensing in the Kingdom

Open data is subject to a license that defines the legal basis for using open data, as well as the terms, obligations, and restrictions imposed on the user. Use of open data also indicates acceptance of the license terms.

Principle 8: Developing a governance model and involving everyone

Open data enables access and participation for all, enhances the transparency and accountability of public entities, and supports decision-making and service delivery.

Principle 9: Comprehensive Development and Innovation

Entities are expected to play an active role in promoting the reuse of open data and providing the necessary supporting resources and expertise. Entities must work in an integrated manner between the relevant parties to empower the next generation of innovators in the field of open data and engage individuals, institutions, and everyone in general in unleashing the capabilities of open data.

4.5.3. Evaluating the value of public data to identify open datasets

The data valuation process to enable the publication of the largest possible amount of open data goes through several main stages, as follows:

Step 1: Identify general data and information

To assess the value of data, the public entity must classify the data (according to the data classification policy) and identify all data sets that can be classified at the “general” level, which may consist of specific files, tables, or records within a database, etc. Next, the benefits, applications, and possible uses of each data set must be identified. The data domain or sector can be taken into consideration when analyzing potential use cases. For example, geospatial data can be leveraged to serve the healthcare sector. Additionally, data sources can be considered: data collected directly by users, data collected automatically through event logs such as electronic transactions, aggregated data, or data developed from other data, etc.

Step 2: Evaluate the usefulness of the data

After identifying data sets in the previous step, the main factors related to data usefulness (usefulness) are studied, which play a major role in assessing its value. These factors include data completeness, accuracy, consistency, timeliness, restrictions imposed on the data, exclusivity to the entity, potential risks of publishing it, and the possibility of accessing and integrating it with other data.

Step 3: Identify potential stakeholders

After evaluating the usefulness of the data in the previous step, all potential stakeholders in the entire value chain are identified. For example, consumer behavior patterns can be disseminated to product manufacturers, not just to retailers. Thus, the parties can identify the main motivations of stakeholders, including generating revenue through developing data products or developing services for the public good, such as those that contribute to improving the quality of life.

After the data value assessment is completed, the stages of the open data lifecycle can begin, as described below.

4.5.4. General rules for open data

The Open Data Policy defines the general rules and obligations that public entities must comply with during the stages of the open data life cycle, including:

Planning for Open Data

Defining Open Data

Publishing Open Data

Update Open Data Monitor

Open Data Performance

Open Data Planning The public authority must:

1. Appointing an open data and information officer in the agency's office, whose primary responsibility is: In support of planning, implementation and reporting on the entity's open data agenda, in line with this policy.

2.Develop an open data plan that includes the following:

Strategic objectives for open data at the agency level.

Identify the data sets of the entity that are required to be published on the National Open Data Platform and prioritize these sets.

Key performance indicators and objectives related to open data for the entity.

Methodology and criteria for prioritizing.

Open data-related training needs. Timelines

for publishing and updating open data.

3.Develop and document the processes required in all stages of the open data life cycle, including:

For example, but not limited to:

Processes for determining which public datasets will be published by the public entity.

Verifying open data compliance with requirements related to information security, personal data privacy, and data quality, regularly reviewing this, and addressing related concerns.

Processes to ensure that data sets are published and updated in the appropriate format and according to the specified schedule, ensuring their comprehensiveness and high quality, and ensuring the exclusion of any restricted data.

Collecting feedback and analyzing performance at the agency level and improving the overall impact of open data at the national level.

4.Ensure that the open data plan is reviewed and updated periodically.

5.Submit an annual report to the Office on the open data plan and the level of progress in achieving the objectives. Open data specified in the plan.

6.Organizing a training course on everything related to open data, with the support of the office or in coordination with it.

7.Launch awareness campaigns to ensure that potential users are aware of the availability of published open data. From the side of the entity, its nature and quality.

Open Data Identification

Public authorities must:

1.Identify all data classified as public data on a regular basis and assess the priority of each.

A set of data sets identified for publication as open data.

2.Assessing the value of the data set and determining the priority of its publication upon receipt of a publication request or when Any dataset that is deemed restricted will be declassified and reclassified as a public dataset.

3.Metadata recording (For specific open datasets and publishing them (Metadata).

4. Study whether combining several sets of open data will lead to a higher level of Classifying data into protected data in accordance with the guidelines issued by the Office in this regard.

Open data publishing

Public authorities must:

1. Publish its open datasets on the National Open Data Platform.
2. Ensure that data is published in standard, unified formats, with a machine-readable structure and is non-proprietary. Formats include, but are not limited to: CSV, JSON, XML, and RDF. Dataset files must be accompanied by documentation related to the format and instructions on how to use them.
3. Provide data in multiple formats whenever possible.

Open data update

Public authorities must:

1. Ensure that all published open datasets are regularly updated according to the mechanism. Specified in the metadata.
2. Continuous review of published data sets to ensure they meet regulatory requirements.

Specific.

3. Ensure that metadata is updated, especially whenever data elements in collections change. Open published data.
4. Maintain data traceability by documenting data sources and maintaining a version history. Data set.
5. Publish open datasets with quality constraints identified and documented in the data

Descriptive.

Open data performance

monitoring Public authorities must:

1. Analyzing the volume of demand for open data and its usage rate to understand the volume of general demand and re- Arrange data sets in order of priority accordingly.
2. Collecting user requests submitted directly or through the National Data Platform Open to publish additional data sets and analyze and respond to such requests in a timely manner.

4.5.5. Roles and Responsibilities

The Open Data Policy defines the following roles and responsibilities at the national and regional levels:

At the national level

1. Office

The Office - as the body responsible for supervising open data initiatives in the Kingdom -

- Coordinating all open data-related initiatives and tasks at the national level. The office determines the strategic direction of open data in the Kingdom and develops national regulations, standards, and procedures that ensure the effective management and dissemination of open data across the Kingdom and the achievement of desired goals.

The office's responsibilities include:

Preparing and reviewing the open data policy- Preparing the open data policy (this policy) And update it, and this policy must be reviewed periodically and take into account potential changes affecting the life cycle of open data.

Developing a plan to adopt an open data policy- Providing continuous guidance to public authorities. To enable the adoption and implementation of this policy.

Open data consultations- Support public authorities to comply with this policy and respond For any inquiries related to identifying, updating and publishing open data.

Measuring compliance with open data requirements: Measuring the extent of compliance of public entities in general Periodically and based on the defined compliance mechanism (please refer to the “Compliance” section for more details) and verify open data initiatives and activities when necessary.

Open data education and awareness: Launching and following up on communication and training initiatives with the aim of: Raising awareness of open data and its adoption at the national level.

Preparing a list of open data: Review of open datasets available at the level National and prepare a list that reflects the extent of progress and achievement.

Open data performance: Analysis of the use of open data and its impact at the national level Finding improvement opportunities to inform the relevant authorities.

Preparing and reviewing open data licenses:A license that allows users to share data. Open, modify and use.

2. National Information Center

The National Information Center acts as the technical operator of the National Open Data Portal, including the design, creation, operation and maintenance of the platform.

The Center's responsibilities include:

Developing, managing, and operating the National Open Data Platform: Platform design and creation And maintain it to ensure that implementing entities are able to publish, manage and update their open data sets. **Granting authorization to participate on the platform and prepare guidelines:**Granting authorization to authorities The public is also required to ensure their access to the National Open Data Platform. This is in addition to preparing and updating operational and technical guidelines for publishing open data on the platform.

Recording platform usage statistics: Recording trends and statistics on the use of open data Published and submitted to the office and public authorities.

At the regional level

The primary responsibility of all public entities is to ensure that their open data is published in accordance with the Open Data Policy. Accordingly, entities must appoint those responsible for implementing open data-related activities as set out below.

The Director of the Authority's Office and the Open Data and Information Officer bear primary responsibility for the Authority's open data activities.

Head of the Authority: The head of the entity - or his delegate - is the person responsible for the practices related to With open data within the entity, his responsibilities include:

Adoption of the open data plan: Approval to implement the open data plan at the entity And supervise it.

Assigning roles related to open data: Assigning different roles related to data Open.

Approval of the annual open data report: Adoption of the annual open data report Prepared by the director of the agency's office.

Director of the agency's office: The strategic director of open data operations in his department is considered, His responsibilities include the following:

Strategic planning for open data: Supervising the development and submission of the open data plan To the head of the entity. He also reviews open data performance, identifies improvement opportunities, and provides guidance on this in the open data plan.

Supervision of open data: Review open data identification activities and arrange them according to Prioritize and approve its publication and ensure the implementation of its updating activities.

Compliance with the Open Data Policy: Ensure that the entity's open data activities comply with For national data policies, including, but not limited to, data classification, personal data privacy protection and freedom of information.

Coordination with the office: The director of the agency's office is the first coordinator between the agency and the office in what follows: Related to open data. Resolves problems related to open data for the entity and escalates them to the office if necessary.

Open Data and Information Officer: He is the operational manager of open data within the entity. His responsibilities include:

Planning for open data: Develop an open data plan, including a methodology for identifying Prioritized open data, setting objectives, and key performance indicators will be agreed upon with the agency's office manager and head of the agency.

Open Data Management: Managing open data activities within the entity, specifically:

- Identify open data
- Sort datasets according to publication priority
- Preparing datasets for publication and documenting metadata
- Publishing open datasets on the National Open Data Platform
- Update, maintain, and quality-check published datasets.

Collecting open data requests: Review comments on relevant open data The authority is responsible for recording and analyzing requests to publish data designated as open data.

Open data education and awareness: Educating and raising awareness among the agency's employees about data Open and support national awareness campaigns in coordination with the director of the region's office.

Coordination with the office (secondary): The open data and information officer In coordination with the office, if needed, as a second level.

Business Data Representative: He is responsible for the following:

Approval of the open data plan: Contribute to the development of the open data plan and management Teams responsible for implementing the plan in coordination with the open data and information officer.

Determine the priority of open data: Providing advice to the open data officer Information on the value of public data sets and the investments required to publish and update them.

Review and approve data sets: Review and approve data sets to ensure accuracy. It meets the specifications specified in the regulations in terms of quality, completeness, and documentation of descriptive data before submitting it for publication.

Business Data Specialist:A member of the Business Data Representative team responsible for:

Identify open data sets: The business data specialist reviews and defines the data. Which are created and processed by the department in which he works on a regular basis and classified as public data if necessary.

Preparing open data sets: Preparing open datasets to be published To ensure that it meets the specifications specified in the policy in terms of quality and completeness, and to document the metadata before submitting it for publication.

Update open datasets: Update published open datasets and related descriptive data.

4.5.6. Compliance

The Office, as the national data regulator, monitors compliance with the Open Data Policy with the support of regulatory bodies.

Compliance Terms

1. All public entities must adhere to the open data policy and submit an annual report. To the office includes, but is not limited to, the following:

   The progress and level of achievement achieved by the entity in its plan, with specific objectives and key performance indicators identified in the open data plan, and the number of open data sets identified.

   Number of open datasets published

2. The regulatory authorities - after coordination with the office - prepare the mechanisms, procedures and controls. Related to the settlement of disputes related to open data, according to a specific time frame and according to the organizational sequence.

3. The office reviews the annual reports prepared by public authorities on: General compliance with the open data policy and sharing it with relevant parties.
4. The office conducts audits periodically or randomly to verify the entity's compliance. Public and review decisions related to publishing or refusing to publish data and take the necessary measures in this regard.

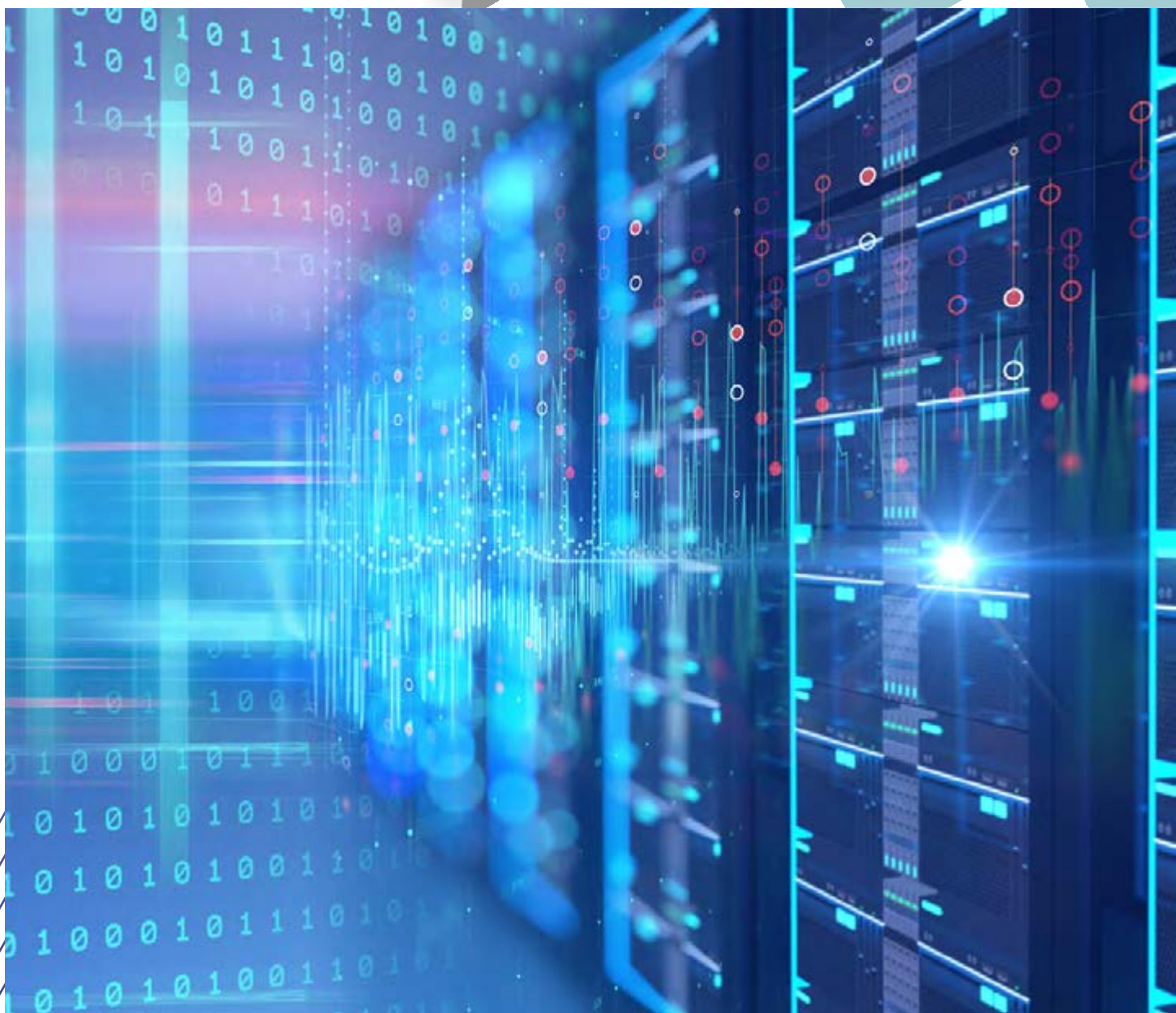
Dealing with non-compliance

When reviewing cases of non-compliance, the office must follow a gradual methodology to analyze the cause of the non-compliance and the extent of the resulting impacts and risks, and deal with these cases according to the following levels:

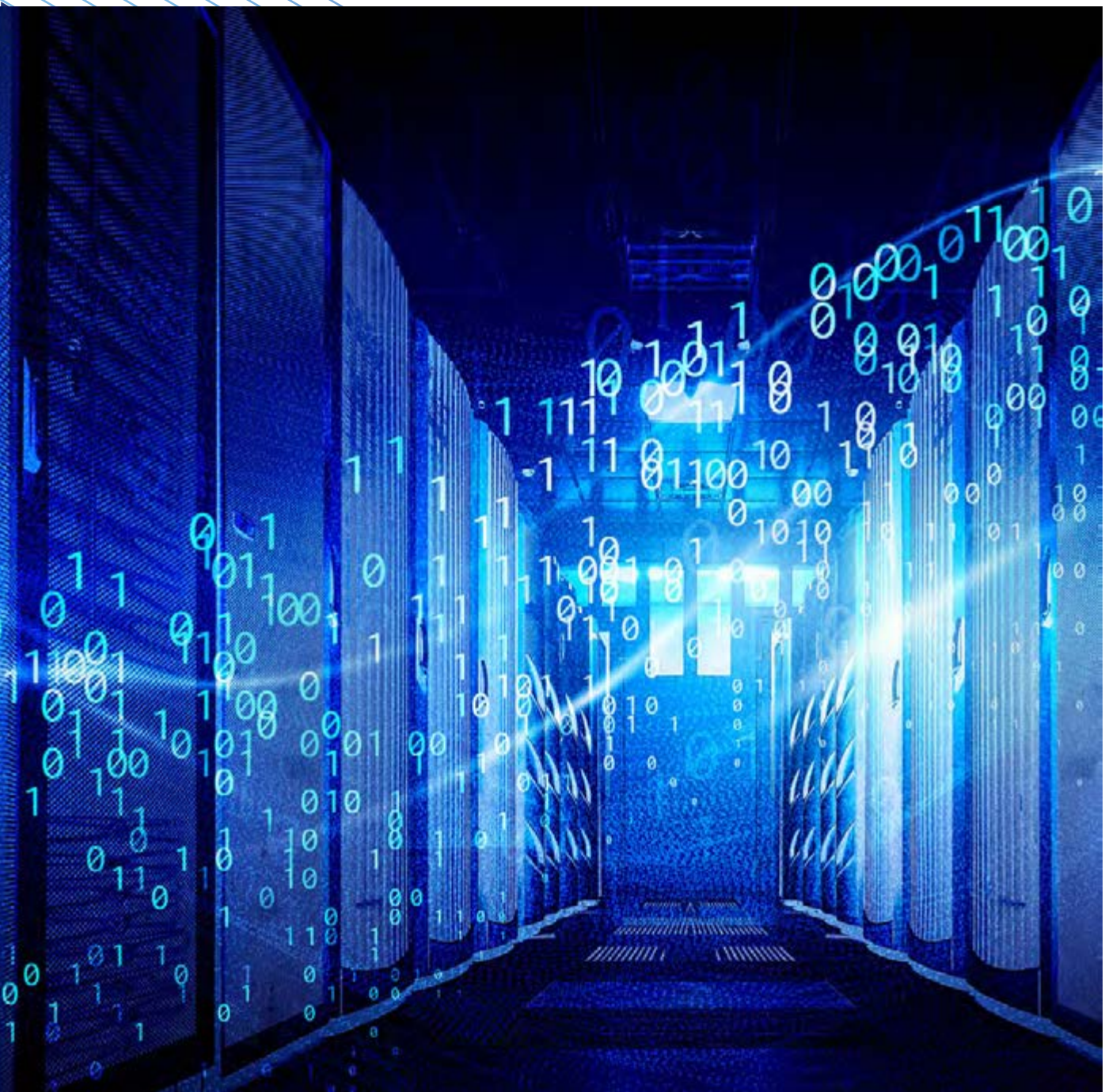
Awareness The office uses awareness when dealing with occasional cases of non-compliance. Or unintended ones with very limited negative effects.

Cooperation The office cooperates with the public authority to prevent, deter or address cases of non-compliance. Compliance with limited negative effects resulting from negligence and non-compliance with the provisions and rules of this policy.

Direct intervention The office investigates ongoing and repeated cases of non-compliance. Or intentional or with severe negative effects and taking decisions that are proportionate to the size and nature of the negative effects.



Personal Data Protection Policy for Children and Those in Their Care



This policy includes the rights and general rules that entities covered by the scope of application of this policy must observe and adhere to in order to limit incorrect practices related to the processing of personal data of children and those in a similar position, and to ensure their protection from negative impacts and potential risks, in addition to preserving their privacy and protecting their rights.

4.6.1. Scope

The provisions of this policy apply to all entities in the public and private sectors, as well as non-profit entities that collect and process the personal data of children and those in a similar situation, in whole or in part, and by any means, whether manual or electronic. The provisions of this policy also apply to all entities
- Outside the Kingdom - which collects personal data of children and those in their position residing in the Kingdom via the Internet.

4.6.2. Rights of children and those in a similar position regarding the processing of their personal data

The child and anyone deemed to be a child shall enjoy all the rights of the data subject stipulated in the Personal Data Protection Policy issued by the Office, and these rights shall be exercised by the guardian.

The child and those in a position of authority also have the right to request the destruction of their personal data after reaching the legal age or the end of guardianship, if the consent to the collection and processing of their personal data was provided by the guardian.

4.6.3. General Rules

Without prejudice to the general rules stipulated in the Personal Data Protection Policy, the controlling authority is committed to the following additional rules that ensure the preservation of the privacy of children and those in their care and the protection of their rights:

1. The controlling authority shall be responsible for preparing and implementing policies and procedures related to data protection. Personal identity for children and those in a similar situation, and the first official in the entity - or his delegate - shall be responsible for approving and adopting it.
2. The controlling authority is committed to assessing the negative impacts and potential risks of all treatment activities. Personal data of children and those in a similar situation, taking into consideration their interests, rights, and all matters related to their family circumstances. The evaluation results shall be presented to the entity's senior official - or his/her delegate - to determine and approve the level of risk acceptance.

3.The controlling authority is committed to reviewing and updating contracts, service level agreements and operations in accordance with Policies and procedures related to the protection of personal data of children and those in their position approved by the entity's senior management.

4.The controlling entity shall undertake to prepare and document the necessary procedures to manage and address privacy violations related to: With regard to children and those in their care, defining the tasks and responsibilities related to the specialized work team, and the cases in which the regulatory body and the office are notified according to the administrative hierarchy based on measuring the severity of the impact.

5.The controlling authority is committed to preparing awareness programmes to enhance the culture of privacy and raise the level of awareness in this regard. Relating to the collection and processing of personal data of children and those in a similar situation.

6.The controlling authority is committed to preparing and developing a clear and accurate privacy notice in a language appropriate to this The category and publish it on the website or the special application (according to the guidance manual for developing the privacy notice issued by the office) and notify the guardian - in a manner appropriate to the time of data collection - of the purpose, the regulatory basis or actual need, and the means and methods used to collect, process and share the personal data of children and those in their position, as well as how to exercise rights, security measures to protect their privacy, and any material changes that occur to it.

7.The controlling authority is obligated to notify the guardian of other sources that are used in the event that data is collected. Additional data indirectly (from other parties).

8.The controller is obliged to provide the guardian with the available options regarding the processing of personal data. For children and those in a similar situation, and the mechanism used to exercise these choices, including, for example, personal preferences through which one can express the desire to share their data for other purposes.

9.The controlling authority is committed to adopting the concept of privacy by design and by default - ensuring a level of Protection without direct intervention from the child or someone of similar status - when providing services specifically targeting this category.

10. The controlling authority is obligated to obtain the guardian's consent – which can be verified after making reasonable efforts – To process personal data of children and those in a similar situation after determining the type of consent (explicit or implicit) based on the nature of the data and the methods of collecting it.

11. The purpose of collecting personal data of children and those in their position must be consistent with the regulations. Relevant and directly related to the activity of the controlling authority.

12. The data content should be limited to the minimum data necessary to achieve the purpose of Collect it.

13. The collection of personal data from children and those in their care shall be restricted to pre-prepared content. (Explained in Rule 12) and shall be done in a fair manner (direct, clear, safe, and free from deception or misleading methods).

14. The use of data shall be limited to the purpose for which it was collected and for which it was approved. Before the guardian.

15. The controller is committed to preparing and documenting the policy and procedures for retaining personal data of children and In their judgment according to the specific purposes and relevant regulations and legislation.

16. The controller is obliged to store and process personal data of children and those in a similar position within the borders of The Kingdom's geography is to ensure the preservation of national sovereignty over this data, and it may not be processed outside the Kingdom except after the controlling authority obtains written approval from the regulatory authority (in accordance with the general rules for transferring personal data outside the Kingdom's geographic borders), after the regulatory authority coordinates with the office whenever necessary.

17. The controlling entity shall prepare and document a data disposal policy and procedures to destroy data in a manner that is Safe, preventing loss, misuse, or unauthorized access - including operational, archived, and backup data - in accordance with what is issued by the National Cyber Security Authority.

18. The controlling authority is obligated to include provisions for data retention and disposal policies in contracts in the event that: Assign these tasks to other processing entities.

19. The controlling authority is obligated to identify and provide the means through which the guardian can access the data. The personal data of the child and those in a similar position, for review and updating.

20. The controlling authority is obligated to verify the identity of the guardian before granting him access to the child's personal data. And those in a similar position, in accordance with the controls approved by the National Cyber Security Authority and the relevant authorities.

21. It is prohibited to share the personal data of children and those in a similar situation with other parties except in accordance with the purposes. Specified after the guardian's approval and in accordance with relevant regulations, rules and policies, provided that other entities are provided with policies and procedures related to the protection of personal data of children and those in their position and included in contracts and agreements.

22. The controlling authority is obligated to notify the guardian and obtain his approval in the event that data is shared with other parties. For use for purposes other than those specified.

23. The controlling authority is obligated to notify the guardian in the event of a desire to communicate with the child or someone of similar status. In a direct manner for any purpose and giving him the opportunity to refuse this communication, while clarifying how he will do so.

24. The controlling authority is obligated to obtain the office's approval – after coordination with the regulatory authority – before participating. Personal data of children and those in similar situations with other entities outside the Kingdom.

25. The controlling authority is prohibited from collecting personal data from a child or someone similar to him that relates to any of the individuals His family in any case, except for the personal data of the guardian.

26. The controlling authority is committed to the requirements of protecting the privacy of children and those in their position from the early stages. Designing services and products that target this category, including websites or digital applications.

27. The controlling authority is committed to implementing appropriate measures that prevent children and those in their position from having access to Their personal and sensitive data is made available to the public in a way that allows them and their families to be directly identified.

28. The controller is obliged to implement appropriate and reasonably practicable measures to delete data. Screening of personal and sensitive posts by children and those in similar situations before publishing them, including displaying personal files and publishing via social media accounts.

29. The controller is committed to not making automated decisions based on the processing of children's personal data. In its ruling and use for various purposes, it has a great impact on them, including, for example, direct marketing.

30. The controlling authority is committed to using adequate administrative controls, technical measures and legal safeguards. To protect the personal data of children and those in their care.

31. The controller is committed to monitoring compliance with policies and procedures related to the protection of personal data. For children and those in their position on a regular basis, and it is presented to the first official in charge of the entity - or his delegate - and the corrective measures that will be taken in the event of non-compliance are determined and documented, and the regulatory body and the office are notified according to the regulatory hierarchy.

4.6.4. Exceptions

1. It is not necessary to obtain the guardian's approval if the service is provided to a child or someone of similar status. It is a preventive or advisory service in accordance with the tasks and competencies of the controlling authority (the authorities concerned with child protection), provided that the authority is committed to collecting the minimum data necessary to achieve the purpose, and destroying it immediately after the completion of the service provision.

2. It is not necessary to obtain the guardian's consent in the event that his personal data is disclosed to a third party. In order to implement a legitimate obligation on the controlling authority, or to implement another system, or to implement an agreement to which the Kingdom is a party, or if the authority to which the disclosure will be made is a judicial or security authority.

3. Guardian consent is not required when the sole purpose of collecting contact information is: The child or someone similarly entitled to it is to respond directly to a specific request from the child or someone similarly entitled to it. This data is not used to contact the child again or for any other purpose, and it is not disclosed. The controlling authority deletes it from its records immediately after responding to the child's request.
4. The guardian's consent is not required when the purpose of collecting the guardian's contact information is The child and those in a similar position are directly responded to – once or more – the specific request of the child and those in a similar position, and this data is not used for any other purpose, nor is it disclosed or combined with any other data, and the guardian is provided with a notification of this.
5. The guardian's consent is not required when the purpose of combining the child's name and the names of those in it is... The guardian's name, contact information, and the protection of the child's safety and those in a similar position are all matters that must be adhered to. This information shall not be used or disclosed for any purpose unrelated to the child's safety and those in a similar position. The controlling authority must provide the guardian with notification of this.

4.6.5. General Provisions

Firstly: The regulatory body shall align the provisions of this policy with its regulatory documents and disseminate it to all The entities affiliated with the authority or linked to it in a way that achieves integration and ensures the achievement of the desired goal of preparing this policy.

secondly: The Regulator is committed to monitoring and documenting compliance with this Policy on a regular basis.

Third: The controlling entity is committed to complying with this policy and documenting compliance in accordance with the mechanisms and procedures that Determined by regulatory authorities.

Fourth: The controlling authority is obligated to inform the regulatory authorities immediately and without delay and no later than (72) Hours from the occurrence or discovery of any incident of personal data leakage, in accordance with the mechanisms and procedures determined by the regulatory authorities.

Fifth: When contracting with other processing entities, the controller is obligated to periodically verify compliance with Other parties shall have this policy in accordance with the mechanisms and procedures determined by the regulatory body, provided that this includes any subsequent contracts concluded by the body.

Sixth: The Office exercises the roles and duties of regulatory bodies over the controlling body that is not subject to regulatory bodies. Organizational.

Seventh: The regulatory authority has the right to establish additional rules for processing specific types of personal data. For children and those in their care, according to the nature and sensitivity of this data, after coordination with the office. **Eighth:**The regulatory body is committed - after coordination with the office - to preparing the mechanisms and procedures that regulate The process of handling complaints and objections according to a specific time frame and according to the organizational hierarchy of the authorities.

4.6.6. Special provisions relating to the legal guardian

1.The controlling authority may obtain the personal data of the guardian directly from the child or someone in a similar position. Provided that you are committed to obtaining the minimum necessary information - name and method of contacting the guardian - only for the purpose of notifying the guardian and obtaining his approval.

2.The controlling authority is committed to using appropriate means to verify the identity of the guardian before obtaining his consent. Granting him access to the child's personal data and those in a similar position, in accordance with the controls approved by the National Cyber Security Authority and the relevant authorities.

3.If the guardian's approval is requested and he does not provide his approval within (10) Within days of contacting him, the controlling authority is obligated to destroy the personal data of the child and those in a similar position, and the data of the guardian that was collected.

4.The controller is obligated not to use the guardian's personal data for any purpose other than that for which it was collected. Within the limits of consent to collect and process personal data of the child and those in a similar position.

5.The controlling authority is obligated to notify the guardian of the requests submitted by the child or those in his position with regard to: With his personal data and obtain his consent.

General rules for transferring personal data abroad

Geography of the Kingdom

4.7. General rules for transferring personal data outside the geographical borders of the Kingdom

The Kingdom seeks to establish policies and standards for the transfer of personal data outside the Kingdom's geographical borders, ensuring the preservation of national sovereignty over this data, as well as the preservation of the privacy of personal data owners and the protection of their rights by defining the obligations of the controlling and processing authorities regarding the transfer of personal data outside the geographical borders, providing appropriate means that enable data owners to exercise their rights, and defining the roles and responsibilities of these entities in addition to To the regulatory and supervisory authorities for the implementation of the provisions of these policies.

4.7.1. Scope

The provisions of this document apply to all public and private entities, as well as non-profit entities in the Kingdom - covered by the scope of application of the Personal Data Protection Policy - that transfer personal data to other entities outside the geographical borders of the Kingdom for the purpose of processing it, with the exception of the transfer of personal data directly to and from individuals.

4.7.2. Data Subject Rights

With reference to the Personal Data Protection Policy, the basic principles of protection grant individuals specific rights regarding the processing of their personal data, while the obligations of controllers define the general rules that must be adhered to when processing it. With regard to the cross-border transfer of personal data, the data subject has the same rights as those set out in the Personal Data Protection Policy, with emphasis on the following rights:

- **Firstly:**The right to information, including notification of the legal basis or actual need to transfer his personal data. Outside the geographical borders of the Kingdom, the place where it is stored or hosted, the parties to whom his personal data will be disclosed when transferred, the purpose of this transfer, obtaining his consent to that, and the security measures taken to protect his personal data during and after the transfer.
- **Second:**The right to withdraw his consent to the processing of his personal data outside the borders - at any time - The purpose of transferring the data was not to achieve the public interest, protect the vital interests of individuals, or implement regulatory requirements.
- **Third:**The right to access his personal data with the external controller/processor, and that To review it, request its correction, completion, or updating, request the destruction of what is no longer needed, and obtain a copy of it in a clear format.

4.7.3. Obligations of the parties

The principle of processing is that it should be within the geographical borders of the Kingdom, where the entity stores and processes personal data within the Kingdom to ensure the preservation of national sovereignty over this data and the protection of the privacy of its owners. It is not permissible to transfer or process it outside the Kingdom except after verifying the cases explained below according to the following sequence:

1. If the external processing entity is entrusted with the processing of personal data in a country within The approval list, the controlling authority/internal processing authority obtains written approval from the regulatory authority for the transfer of data, and the regulatory authority coordinates with the office.
2. If the external processing entity is in a country that is not on the accreditation list, the transfer of personal data Outside the geographical borders of the Kingdom requires an adequate level of protection - no less than the level of protection guaranteed by the Personal Data Protection Policy issued by the Office - after conducting an assessment of the level of protection provided by the external processing party.
3. If there is not an adequate level of protection, the authority shall put in place appropriate safeguards to protect the rights of Data owners, for example, use standard clauses or binding rules.
4. If the entity is unable to provide sufficient guarantees, it may rely on one of the statutory exceptions. Which requires transferring data and is explained in Clause (Third) below.

In all cases mentioned in paragraphs (2), (3) and (4) above, the internal controller or processor must obtain written approval from the regulatory authority to transfer the data, and the regulatory authority must coordinate with the office.

First: Assessing the level of protection

The entity wishing to transfer data across national borders must conduct a case-by-case assessment of the potential impacts and risks to determine whether the external controller/processor will provide an adequate level of protection for the rights of data subjects and present the results of the assessment to the entity's chief executive to determine and approve the level of risk acceptance. To do this, the entity must adhere to evaluation standards, whether general or legal, to ensure that the level of protection is appropriate in all circumstances:

A- General evaluation criteria

- Nature and sensitivity of the data: When assessing the level of protection, the entity must take into consideration the type of The value and volume of the data to be transferred and its degree of sensitivity, as transferring sensitive personal data requires a high level of protection.

- Purpose of data processing: When assessing the level of protection, the entity must take into consideration: The purpose of processing, the target group of data subjects, the scope of processing, and the parties with whom the data will be shared, as processing sensitive personal data on a large scale requires a high level of protection.

- The period during which the data is processed: When assessing the level of protection, the entity must take into consideration: Consider whether the processing will be carried out on a restricted or occasional basis – just once or for a limited period – or on a frequent and regular basis, as personal data that will be processed on a regular and long-term basis requires a high level of protection.

Data source: When assessing the level of protection, the entity must take into consideration the country in which it is located. The data was collected from - not necessarily the country from which the data will be transferred - in order to determine the expectations of the data subjects regarding the level of protection, as transferring personal data collected from countries subject to a very high level of protection requires a level no less than the level of protection in these countries.

- Final destination of data: When assessing the level of protection, the entity must take into consideration: The stages through which personal data is transferred – which may sometimes involve more than one country – and an assessment of the level of protection in the country that is the final destination – the last stage of the transfer.

- Security controls: When assessing the level of protection, the entity must take into account the procedures: Administrative and technical measures and physical controls adopted in the entity's information security policies, such as encryption, security controls and international standards.

If the results of the protection level assessment – based on general criteria – show that, in the specific circumstances of the case, the negative impacts on the rights of data subjects are limited and the potential risks are low, then the protection level assessment – based on legal criteria – may not be necessary in this case.

B- Legal evaluation criteria:

The entity wishing to transfer data across national borders must take these criteria into account when the results of the assessment of the potential impacts and risks in paragraph (a) above are not sufficient, and in such cases, for example, sensitive personal data are transferred on a permanent, regular and large scale.

- Applicable regulations and legislation: When assessing the level of protection, the entity must take into consideration: Whether the country to which the data is to be transferred has systems and legislation that protect the rights of data subjects with regard to the processing of their personal data, and ensure the ability of the participating parties to enter into contracts and abide by these contracts.

- International obligations: When assessing the level of protection, the entity must take into consideration whether: The country to which the data is to be transferred is a party to international agreements or adopts international principles and standards for the protection of personal data.

- Approved rules and practices: When assessing the level of protection, the entity must take into consideration: Whether the country to which the data is to be transferred has rules of conduct, general practices or specific standards for the protection of personal data.

Second: Appropriate guarantees

If the entity is in a country that is not on the accreditation list and has not been subject to a protection level assessment or if the protection level is insufficient, it must provide appropriate guarantees to protect personal data, including:

- Standard contractual terms: The entity must include standard clauses in contracts and agreements. Or standard - approved by the office - to restrict the transfer of personal data outside the Kingdom's geographical borders, ensuring the preservation of the privacy of its owners and the protection of their rights.

- Common binding rules: The controlling entity and the processing entity – each separately – that operates A multinational group shall develop legally binding internal common rules applicable to cross-border transfers of personal data, including handling and notification of privacy breaches, which shall be approved by the Office. These common rules shall be included as an annex to service level agreements or contracts concluded between the two parties. The controlling entity must also obtain the approval of the regulatory authority if there is any legal obligation to which this entity or one of its affiliates is subject in another country that is likely to have a negative impact on the guarantees provided by the binding common rules.

- Approved rules of conduct: That the authorities use the codes of conduct approved by the authorities. The regulatory or office as an effective tool that defines the obligations of the controlling and processing entities to ensure the preservation of the privacy of data owners and the protection of their rights.

- Accredited certificates: That the authorities seek the assistance of independent external parties to issue certificates. Accreditation confirms that appropriate safeguards are in place by the controllers or third-party processors. These entities also provide enforceable commitments to implement these safeguards, including provisions related to data subject rights.

- Binding agreements between public authorities: That public authorities - whether they are controlling authorities - Or processing entities - by signing a legally binding agreement to transfer personal data, provided that this agreement includes binding contractual clauses that guarantee the preservation of the privacy of data subjects and protect their rights.

Third: Exceptions for specific cases

Entities may transfer personal data outside the geographical borders without being bound by the terms and conditions set forth in Clause (First) and Clause (Second) above in specific cases, including that the data transfer is outside the geographical borders of the Kingdom:

1. Based on data subject consent.
2. In implementation of a contractual obligation to which the data subject is a party.
3. In compliance with judicial requirements.
4. In implementation of the provisions of another law or international agreement to which the Kingdom is a party.
5. To preserve the public interest, including the protection of public health or safety.
6. To protect the vital interests of data subjects.

In all cases mentioned in paragraphs (1), (2), (3), (4), and (5), the internal controller or processor must obtain written approval from the regulatory authority for the transfer of data – each case separately – and the regulatory authority must coordinate with the Office. As for the case mentioned in paragraph (6), the controller or processor must notify the regulatory authority only, and the regulatory authority must notify the Office thereof.

4.7.4. General Provisions

Firstly: Regulatory authorities shall harmonize this document with their regulatory documents and circulate it to all Its affiliated or related entities, in order to achieve integration and ensure the achievement of the desired goal of preparing these rules.

Second: Regulatory authorities monitor the compliance of their affiliated or related entities with these rules in a comprehensive manner. periodic.

Third: Controlling entities and processing entities must comply with these rules and document compliance in accordance with the mechanisms. And the procedures determined by the regulatory authorities.

Fourth: When contracting with processing entities – inside or outside the Kingdom – the controlling authorities must ensure that: Periodically, the processing entities comply with these rules in accordance with the mechanisms and procedures determined by the regulatory authorities, including any subsequent contracts concluded by the processing entities.

Fifth: The Office exercises the roles and duties of regulatory bodies over control bodies that are not subject to regulatory bodies. Organizational.

Sixth: Regulatory authorities may establish additional rules for the transfer of specific types of personal data. According to the nature and sensitivity of this data, after coordination with the office.

Seventh: The Office reviews the evaluation criteria - general and legal - related to data protection. The personality when transferred outside the geographical borders of the Kingdom and taking the decisions regulating it.

Eighth: The Office develops a specific list of key factors that determine the appropriate level of protection. These include, for example, regulations and legislation, the protection of rights and freedoms, national security, rules for the protection of personal data, the supervisory authority for data protection, and binding obligations undertaken by the state.

Ninth: The office prepares, reviews, publishes and updates the accreditation list periodically, based on: To assess the appropriate level of protection, so that it is not less than the level of protection guaranteed by the personal data protection policy issued by the office.

Tenth: The Office prepares and reviews standard clauses to protect personal data.


0,64 0,69 0,63 0,65 0,60
0,67 0,72 0,65 0,68 0,62 0,60 0,59
0,24 0,29 0,28 0,23 0,22 0,18 0,21 0
0,30 0,35 0,34 0,29 0,28 0,24 0,27 0
0,36 0,41 0,39 0,35 0,33 0,29 0,32 0

Policies not approved by the Board of Directors

5. Unapproved policies n before the Board of Directors

In addition to the seven national data governance policies, two additional policies are being worked on but have not yet been approved by the Board of Directors:

1. Data Monetization Policy

It includes a set of principles, rules and obligations for the various parties involved in data marketing in order to achieve revenues from data and data products.

2. General rules for data governance when developing or using AI systems

Assisting entities in using standard criteria and ethics when building and developing solutions based on artificial intelligence technologies, developing and using them responsibly, ensuring the preservation of the privacy of personal data owners, and protecting their rights related to the collection and processing of their data.

Data Monetization Policy

5.1. Revenue generation policy from the Data

The Kingdom seeks to benefit from the vast amount of data collected, produced, or handled by entities in the public and private sectors, in addition to non-profit entities, to improve performance efficiency, increase productivity, facilitate the provision of services in creative and innovative ways, enhance economic development, and improve the quality of life by conducting accurate forecasts, anticipating the future, supporting the decision-making process, enabling leadership and innovation, and creating qualitative investment opportunities in a number of Different fields.

5.1.1. Scope

The provisions of this policy apply to any marketing of government data or products based on this data, whether partially or fully processed. Private sector data, as well as any activity related to collecting, processing, and developing any private sector data product, are excluded from the scope of application of this policy.

5.1.2. Related Policies

All entities covered by the scope of application of this policy are committed to complying with relevant regulations, rules, and policies, including the national data governance policies issued by the Office and approved by the Board of Directors of the Saudi Data and Artificial Intelligence Authority, including specifically the policies explained below, which specify the obligations of data providers when generating revenue from data or data products:

1. **Data Classification Policy:** This policy aims to establish a unified national framework for data classification.
   - Produced or processed by government agencies - regulates the right to access this data and the mechanism for dealing with it.

2. **Personal Data Protection Policy:** This policy aims to establish general rules and regulations. Which regulates the collection and processing of personal data.
3. **Data Sharing Policy:** This policy aims to promote the principle of sharing key data that Produced by government agencies to achieve integration and adopt the one-time principle of obtaining data from its correct sources, reducing duplication, conflict, and multiple sources.
4. **Freedom of Information Policy:** This policy aims to regulate the right to access or obtain data. Unclassified as one of the degrees of confidentiality produced by government agencies, which enhances the integrity and transparency system.

5. **Open Data Policy:** This policy aims to make available a specific set of data. Unclassified information produced by government agencies for researchers, entrepreneurs, innovators, and startups, ensuring a favorable environment for business growth.
6. **National data management controls and standards:** This document aims to determine the minimum Specifications and controls related to each of the main areas of data management to maximize the benefit of national data.

5.1.3. Basic principles of data monetization

Principle 1: Data is a national asset

The data produced by government agencies are considered one of the national assets that these agencies must manage in a way that achieves the public interest in accordance with Cabinet Resolution No. (40) dated 27/2/1427 AH, which stipulates in paragraph (1) that government information and data are considered a national wealth, and all government agencies must develop them. To ensure their preservation as national assets, the government agency reserves the intellectual property rights to the data, and it is not permissible for them to be used by any party. Other than pursuant to a data sharing agreement between the parties. As for data products, any party that has developed a product based on data has the right to retain the intellectual property rights developed in accordance with the relevant systems and regulations.

The second principle: revenue development

Data is a valuable asset that can be leveraged to increase spending efficiency and grow data-related revenues to ensure the sustainability of services provided by government agencies.

Principle 3: Privacy by Design

Taking into account privacy requirements from the early stages of data and data product revenue generation processes in accordance with the Personal Data Protection Policy.

The fourth principle: The origin of data is availability.

The marketing of raw data or data products should not conflict with the open data policy and the efforts made by government agencies to enhance their contribution to open data initiatives and strategies.

Principle 5: Promoting a culture of participation

Marketing of unprocessed data or data products must not conflict with the data sharing policy and efforts to achieve integration between government agencies and obtain data from its correct sources.

Principle 6: Preventing monopolistic practices

Government agencies play a key role in shaping the data market and encouraging innovation in the private sector. Therefore, government agencies must restrict any unfair advantage (including monopoly), promote equal access to data, and remove barriers that hinder the development of data products by the private sector, leading to a fair and competitive data market.

The seventh principle: transparency

Information related to revenue recognition data must be documented and made available when needed. This includes, but is not limited to, the revenue recognition model, data used, approved pricing model, and revenue collection.

Principle 8: Cost Recovery

Government entities shall strive to achieve the minimum possible profit from data or data products, while maintaining their role as market creators and economic developers in accordance with Principle 6. Government entities shall also adopt a cost-recovery pricing model unless the return on investment or market price is not justified.

5.1.4. Revenue Generation Policy Framework – General Rules

In line with the scope of application of this policy, a framework has been developed to regulate the realization of revenue from unprocessed data and data products. Revenue can be realized in one of the following ways:

Sharing raw data for a fee. Providing insights or analytics.

Offering a product or service such as: analytics platforms.

Revenue generation models

A revenue model is the structure that defines the revenue generated by a business model, encompassing the value-added product or service and the target consumers. Accordingly, there are several common models, each with varying uses depending on the nature of the product or service. These include, but are not limited to, advertising, competitive advantage, licensing, commissions, and other models.

Pricing models

Pricing Model: The mechanism used to determine estimated prices for data and data products. Accordingly, there are a number of models used depending on the revenue generation model and the product or service, including, for example:

1. **Commercial Pricing Model (Profit Achievement):** Estimating the price of data and data products based on The price of similar products or services in the market.
2. **Marginal Cost Model:** Data provisioning costs calculation For another beneficiary, it is usually close to zero, or equivalent to providing it for free.
3. **Cost Recovery Form:** Marginal cost plus calculation Costs of providing data or developing data products.
4. **Cost Recovery + ROI Model:** Data provisioning costs calculation Or data products, in addition to determining a specific percentage as a return on investment, which allows for cost recovery and adding a profit margin on value-added services.

To achieve the desired goal of this policy, the two models referred to in paragraph (3) and paragraph (4) above are considered the pricing models approved by the Office when government agencies generate revenues from data or data products.

Revenue Realization Framework

The data revenue framework includes three main tracks, each of which describes the rules related to data revenue generation and data products. To ensure fair competition and prevent monopolistic practices, government entities must adhere to the following:

Making available the largest possible amount of classified data (at the general level) and publishing it as open data - free of charge and without charge - in accordance with the open data policy prepared by the office. Sharing its data and making the shared data available electronically free of charge (without charge) to other beneficiary government agencies, in implementation of Royal Decree No. 17850 dated 3/16/1441 AH.

The first track: Table (1) below shows the obligations of government agencies towards government agencies (G2G).

	Other than that Toprocess	Productive T Data
	Free	Recover the yÂlif
Data The classified (restricted , general)	Free	Recover the yÂlif

Table 1 Obligations of government agencies towards government agencies

General rules related to the first track

1. Government agencies do not charge fees for unprocessed data, whether when open data is made available. Or when sharing classified data (at the level of: restricted or public) with other government agencies to implement the tasks and responsibilities assigned to them. This rule also ensures compliance with the Royal Decree No. 17850 dated 16/3/1441 AH - referred to above.
2. Government entities can generate revenue from data products developed from open data. Or classified data (at the level of: restricted or general), provided that these products are provided by the private entity or entities, and pricing is in accordance with the cost recovery model stipulated in this policy.
3. Government agencies are committed to the provisions of the data sharing policy and personal data protection requirements when... Developing data products, including, for example, pre-processing personal data before sharing it, such as: Data Masking, Data Scrambling, or Data Anonymization.
4. Government agencies must provide, in accordance with the sixth principle, equal access to any data or A data product used to generate revenue by private entities in order to achieve fair competition and prevent monopolistic practices.

The second track Table (2) below shows the obligations of government agencies towards private entities or individuals (G2B/G2I)

	Unprocessed data	Data Products
	Free	Cost recovery
Classified data (Restricted, General)	Cost recovery	Cost Recovery (Plus)

Table 2: Obligations of government agencies towards private entities and individuals

General rules for the second track

1. Government agencies do not impose fees on open (unprocessed) data that is made available to the public (government agencies). Private and individuals).
2. Government agencies can generate revenue from data products developed from open data, on the These products shall be provided by the private entity or entities, and pricing shall be in accordance with the cost recovery model stipulated in this policy.
3. Government entities can generate revenue from unprocessed, classified data (at the level of: restricted or (General), provided that this data is provided by the private entity or entities, and pricing shall be in accordance with the cost recovery model stipulated in this policy.
4. Government entities can generate revenues from data products (processed data) classified (on Level: Restricted or General), provided that these products are provided by the private entity or entities, and pricing is in accordance with the cost recovery model (Plus) stipulated in this policy.
5. Government agencies are committed to the provisions of the data sharing policy and personal data protection requirements when Sharing unprocessed data or developing data products, including, for example, pre-processing personal data before sharing it with private parties or individuals, such as masking, scrambling, or anonymization.
6. Government agencies must provide, in accordance with the sixth principle, equal access to any data or product. Data used to generate revenue by private entities or individuals in order to ensure fair competition and prevent monopolistic practices.

The third track: Table (3) It clarifies the obligations of private entities towards government entities, private entities and individuals (B2G/B2B/B2I) in accordance with the policies issued by regulatory authorities, the Office and other relevant entities, including, for example, the General Authority for Competition.

	notA no process	Productive Data
	Not subject to the provisions of the regulatory guidelines and authorities. For policy, it can be organized. hApproved by the relevant Dauthorities	Not subject to the provisions of According to the recommended guidelines of the relationship Policy, regulatory bodies hand pricing models can hbe regulated. Maha Show at
Government data which are dealt with by the authorities **Private (restricted, public)**	Cost Recovery (2G B) Cost recovery S (B2B/B2I)	Cost recovery (b) tQ)
Authority data Private	Not subject to the provisions of According to the models of endeavour Politics, and can be identified RRecommended business from Regulatory bodies and relevant authorities	Not subject to the provisions S of commercial pricing models Y Regulatory and relevant authorities Dry, and can be identified and Q Recommended by relevant authorities

Table 3: Obligations of private entities towards government agencies, private entities and individuals

General rules for the third track

1. Private entities can generate revenue from data products developed from open data, Note that the pricing of data products is not subject to the provisions of this policy, but rather to the pricing models recommended by regulatory and relevant authorities, including, for example, the General Authority for Competition.

2. Private entities are not permitted - if they are granted a license to use data by a government agency - Reusing unprocessed government data for purposes other than those specified in data-sharing agreements or sharing it with other entities, whether for a fee or free of charge. This rule applies to all private entities, including commercial agreements that govern the relationship between the private entity and the government entity.

3. Private entities can generate revenue from unprocessed data obtained from Government entities classified (at the level of: restricted or general) when participating with other government entities, provided that the pricing is in accordance with the cost recovery model stipulated in this policy.

4. Private entities can generate revenue from data products obtained from third parties. Government classified (at the level of: restricted or public) when presented to other private entities or individuals, provided that the pricing is in accordance with the cost recovery (plus) model stipulated in this policy.

5. The Data Office recommends that regulatory bodies coordinate with relevant authorities to determine: Pricing models that can be used by private entities to prevent monopolistic practices and achieve fair competition.

5.1.5. Pricing Model (Cost Recovery)

Data Pricing Standards

In order to price data and data products in accordance with the pricing models described in this Policy, the following factors are taken into consideration:

Data scarcity (raw or primary data, number of data creators, etc.)

Multiple data sources (the number of data sources through which data is linked or collected to provide insights and analysis, the extent of exclusivity of these sources, the size of the fields, etc.)

Number of subscribers/customers for the entity (diversity of segments, etc.)

Data value (nature and content of data "personal or non-personal, encrypted or unencrypted, aggregated or non-aggregate, etc." Data quality, possible uses, intended beneficiaries, etc. Data type (structured, semi-structured, unstructured data)

Data size (size in GB, number of records, etc.) Data price

and similar data products in the market. Cost recovery

pricing mechanism

Based on the basic principles and general rules explained above, entities should follow the following guidelines to estimate the value of unprocessed data and data products:

1. The entity should take the following factors into consideration when pricing cost recovery:

Price = Data collection costs + Development costs

Data Collection Costs: Costs related to collecting, cleaning, preparing, and maintaining data (hardware, software and applications, human resources, hosting, etc.)

Development cost: The cost related to analyzing, representing, or processing data, in addition to other activities related to developing the data product (hardware, software, applications, human resources, etc.), as well as costs related to direct connectivity.

The entity must estimate the costs of collection and development for each data product separately. Any additional costs incurred must be justified and added to the costs mentioned above.

2. Government agencies have the discretion to price data or data products at less than the refund.

Estimated cost.

3. If a government agency deems it necessary to add a profit margin above the cost recovery, approval must be obtained. From the office after providing it with sufficient justifications.

4. Government agencies determine the price of data or data products in a uniform manner among beneficiaries. Data, and any exception must be submitted to the office for approval.

Roles and Responsibilities

Firstly: The administrative unit/work team responsible for business development and revenue generation in the entity By developing an electronic store or directory that includes the data and data products that you wish to provide or offer, and determining the detailed pricing model for each service or product according to the paths explained above, and sending it to the office of the entity.

Second: The authority's office reviews the services and products displayed in the store or directory to ensure that: The data to be provided or used to develop data products is classified at a restricted or general level, and the privacy requirements are met in accordance with the Personal Data Protection Policy, and detailed pricing models are determined in accordance with the paths described in this policy.

Third: The party wishing to obtain data or data products shall submit the request to The entity's office shall undertake such a sharing in accordance with the steps outlined in the data sharing policy, provided that the entity's office verifies compliance with the provisions of the data sharing policy and the general rules stipulated in the revenue generation policy.

Fourth: The agency's office documents all data sharing requests and related decisions in special records.

5.1.6. General Provisions

Firstly: The data offices in the regulatory bodies shall align the provisions of this document with their regulatory documents. And circulate it to all its affiliated or related entities in a way that achieves integration and ensures the achievement of the desired goal of preparing this policy.

Second: Regulatory authorities are obligated to specify the monitoring tools for collecting revenue from data - in a manner that does not conflict with With the State Revenue System - monitoring compliance with this policy and providing the office with compliance reports periodically.

Third: Every government agency must collect all its revenues from government data, whether it is data Unprocessed or unproductive data shall be recorded in a detailed register, provided that it does not conflict with the State Revenue System and its executive regulations.

Fourth: Each government entity is obligated to obtain official and documented approval for any revenue related to data. The processing or data products are not authorized by the head of the entity or his authorized representative.

Fifth: Without prejudice to the provisions of the State Revenue System, government agencies are obligated to provide the Office and the Ministry of Finance with: With annual reports on its revenues from government data (processed and unprocessed), in the month of December of each year, starting from the first of December of the issuance of this policy.

Sixth: The Office exercises the roles and duties of regulatory bodies over entities not subject to regulatory bodies.

Organizational.

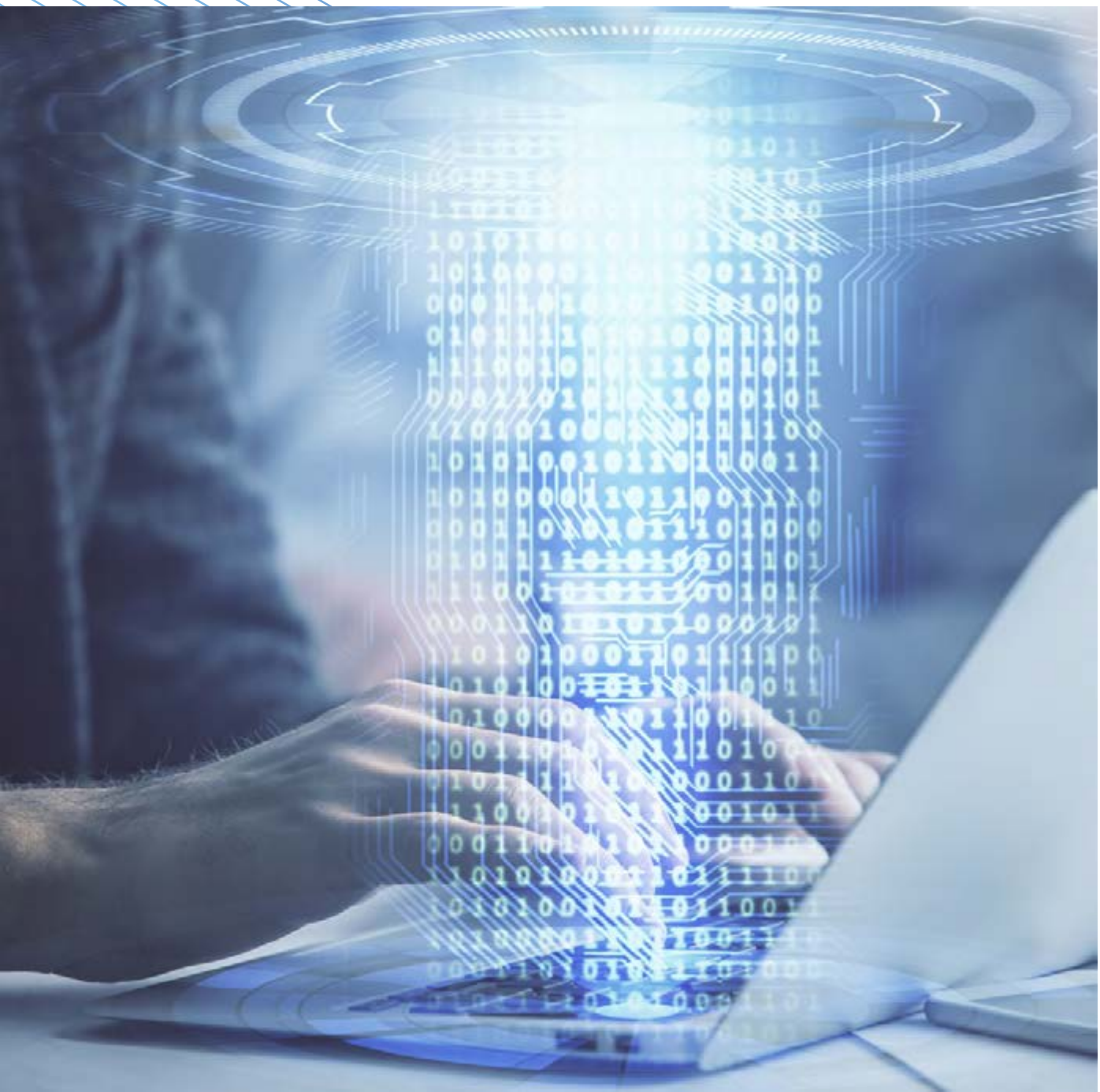
Seventh: Regulatory authorities have the right - after the office's approval - to propose adding some investigation models.

Revenues and setting additional standards to develop pricing models according to the nature of the activities of its affiliates or associated entities.

Eighth: The regulatory authorities, after coordination with the office, prepare the mechanisms and procedures that regulate... The process of handling complaints and disputes related to revenue realization according to a specific time frame and according to the organizational hierarchy.

Ninth: The office, in coordination with the relevant authorities, reviews revenue generation models. Pricing models are periodically updated in line with market requirements, ensuring fair competition and preventing monopolistic practices in the data sector.

General rules for data governance when developing or using artificial intelligence systems



5.2. General rules for data governance when developing or using artificial Intelligenda intelligence systems

It includes the basic principles, general rules, and ethical practices that must be taken into account when using and developing artificial intelligence systems to reduce risks and potential negative impacts and ensure responsible use.

5.2.1. Scope

The provisions of this document apply to all entities in the public and private sectors, in addition to non-profit entities, that collect data, including personal data and data masking, scrambling, or anonymization, by any means, and analyze it using artificial intelligence systems to achieve specific goals.

5.2.2. Basic principles for developing and using artificial intelligence systems The

first principle: justice

The data sample and the data to be analyzed must be chosen fairly and objectively, without any bias or discrimination of any kind, whether racial, ethnic, regional, intellectual, etc. **The second principle:**

transparency

Artificial intelligence systems and predictive models should be built with a high degree of transparency and clarity, in a manner that is explainable and interpretable, while providing the ability to track the stages of making important decisions that were made automatically and that may lead to material or moral damage to the data owner.

Principle 3: Accountability/Responsibility

Artificial intelligence systems and predictive models must be held accountable by assessing the negative impacts and potential risks of their irresponsible development or use, while providing the ability to challenge important decisions related to the interests of individuals.

The fourth principle: inclusiveness

The sample of data and information to be analyzed must be comprehensive, diverse, and fairly represent all segments of society or target groups, without any bias or discrimination.

The Fifth Principle: Humanity

Predictive models should be built using a safe, ethical methodology based on human rights and values to ensure that AI systems are used for the good of humanity.

Principle 6: Security

Artificial intelligence systems must be built in a safe manner that limits the machine's control and control, while providing the ability to control it throughout its lifespan, ensuring that it is not able to cause any harm or damage.

Principle 7: Data Quality

The sample of data or data to be analyzed must be accurate, correct, complete, and relevant to the purpose of its use, while ensuring that it is constantly updated and that its validity and the reliability of its sources are confirmed.

5.2.3. Data Subject Rights

The owner of personal data has the right stipulated in the Personal Data Protection Policy, in addition to the rights related to making decisions by automated means without human intervention (Automated Decisions), including profiling/analysis of psychological and behavioral characteristics of individuals or evaluation of some personal aspects (Proifling), which may result in:

1. Regulatory consequences include the competent authorities taking the necessary measures against him, including: Summoning him, hearing his testimony, requesting verification of his information, and other procedures.
2. Material or moral damages, such as loss of benefit, damage to reputation, or other similar damages.

Accordingly, the owner of personal data has the right not to have decisions made on his behalf automatically except in the following cases, while providing the possibility of tracking the stages of making important decisions:

1. If this is necessary to conclude a contract or implement a contractual obligation, the owner of the personal data is a party. In it
2. If this is in implementation of regulatory requirements in accordance with applicable laws and regulations, or authorized by The office accepts after adopting the necessary controls and procedures to guarantee the rights of the data owner and the legitimate interests of the entity.
3. If this is based on the express consent of the data subject.

In the two cases referred to in paragraphs (1) and (3), the data owner has the right to obtain human intervention from the authority to express his point of view or object to the results and decisions.

5.2.4. General rules for using and developing artificial intelligence applications First: Obligations of AI system developers

1. Take the necessary measures and sufficient steps to ensure the absence of bias when selecting the data sample, including: This bias towards the majority against minorities.

2.Take the necessary measures and sufficient steps to ensure the diversity of the data sample and its representation of all segments. The community or target groups fairly and without any discrimination.

3.Conducting a bias assessment, documenting the results, and having them approved by the official in charge of the entity or his delegate before... Start developing data-driven predictive models and AI algorithms.

4.Do not use sensitive personal data as sample data during the training phase of artificial intelligence systems. Artificial intelligence and its development or predictive models.

5.Not using personal data that leads to identifying the individual specifically without basis It is legal, whether with the consent of the data owner or other legal basis stipulated in the Personal Data Protection Policy, provided that the main purposes for collecting and analyzing this data are clarified.

6.Conduct a privacy impact assessment to evaluate the psychological and social impacts of using personal data. As a sample of data to ensure the preservation of the privacy of its owners and the protection of their rights.

7.Commitment to the principle of transparency when building predictive models based on data and artificial intelligence algorithms Artificial intelligence, by explaining the mechanism of the algorithms used in an understandable and interpretable manner that helps in identifying the reasons behind these models reaching certain results, without conflicting with intellectual property systems or other relevant systems.

8.Take the necessary measures and sufficient steps to verify the accuracy and correctness of the interpretation of the results. Contradictory to avoid misleading measurements.

9.Proving the fairness of important decisions by providing the possibility of verifying the main factors that lead to Making any decision that could affect the vital interests of individuals.

10.Providing a manual intervention mechanism that allows individuals to track the stages of making important decisions related to With their vital interests and object to them.

11.Preparing a mechanism that includes a set of criteria necessary to evaluate the reliability of AI systems. Artificial intelligence in predicting and making future decisions.

12.Adopting a comprehensive methodology for testing the quality of systems and predictive models based on data and algorithms. Artificial intelligence according to standard practices.

13.Take the necessary measures and sufficient steps to ensure the quality, accuracy, validity and relevance of the data sample. For the purpose of building predictive models and artificial intelligence systems.

Second: Obligations of users of artificial intelligence systems

1.Preparing policies and guidelines related to supporting and enabling the ethical use of artificial intelligence. According to standard best practices.

2. Commitment to the national data governance policies issued by the Office and approved by the Board of Directors. Saudi Data and Artificial Intelligence Authority.

3. Obtaining the office's approval - after coordination with the regulatory authority - before analyzing the classified data. One of the degrees of confidentiality according to the data classification policy.

4. Data analysis should be limited to the classification levels (restricted, general), provided that it is determined whether There is a need to process data before analyzing it, including, but not limited to, masking, anonymization, and aggregation.

5. Take the necessary measures and sufficient steps to ensure the quality, accuracy and validity of the data to be analyzed. The reliability of its sources, the appropriateness of its collection methods, and its freedom from deception or misleading methods.

6. Providing appropriate channels that enable individuals to obtain explanations related to results and decisions. The mission that affects their vital interests and enables them to object to these decisions or request proof of their justice.

7. Preparing guidelines to explain how predictive models or AI algorithms work. The artificial intelligence used, the data to be analyzed, the target groups, and the factors that influence the results and important decisions.

8. Preparing a detailed record of all data analysis activities, including the history of all operations and procedures. Which was done on each set of data sets.

9. Take the necessary steps to ensure that the machine does not take control and that AI systems make decisions. Acting on behalf of the concerned persons or influencing their decisions without obtaining their prior consent.

10. Preparing and documenting data retention policies and procedures in accordance with the specified purposes, regulations and legislation. Related.

11. Dispose of and destroy data securely – including archived data and backup copies – In accordance with the data disposal policy approved by the entity and in accordance with relevant regulations and policies.

12. Preparing a procedural guide that explains the steps necessary to assess the risks and potential impacts resulting from the analysis. Data is analyzed using predictive models and artificial intelligence algorithms to measure the extent to which public objectives are achieved with the least possible impact on individual privacy.

13. Preparing a procedural guide that explains the steps necessary to assess the impact of bias on results to ensure the diversity of the group. Data to be analyzed and represented fairly for all user categories without any discrimination.

14. The use of data analysis results should be restricted to the purpose for which they were used and should be The purpose is consistent with relevant regulations, rules and policies.

15. It is prohibited to build comprehensive personal records about individuals by collecting data from multiple sources, which It helps in analyzing them and extracting sensitive personal information that may directly or indirectly lead to predicting health, financial, and social conditions, intellectual tendencies and orientations, and other things.

Third: Obligations related to facial recognition technologies

1.Conduct an assessment of the negative impacts and potential risks when determining the purposes related to the use of technologies. Face recognition.

2.The use of facial recognition technologies for the purposes of continuous surveillance – tracking a person's movements – is prohibited. Or a group of people permanently in public places and on a large scale - whether this is momentarily or by referring to historical records, with the exception of its use for specific purposes in accordance with the systems, regulations and policies in effect in the Kingdom.

3.Restricting the use of facial recognition technologies to the minimum amount of data needed to achieve the purposes Specified based on regulatory foundations, specifying the retention period and the parties with whom this data is to be shared.

4.Take the necessary measures and sufficient steps to evaluate the quality, accuracy and relative performance of the built systems. On facial recognition techniques before using them, in accordance with standard practices.

5.The use of body-worn or wearable cameras is prohibited.Body Worn Cameras.

6.Commitment to the principle of transparency and informing individuals in an appropriate manner in the event that there are cameras integrated with technology. Facial recognition in places where the use of these technologies is permitted (such as airports and the headquarters of some government agencies).

7.Preparing and documenting data retention policies and procedures in accordance with the specified purposes, regulations and legislation. Related.

5.2.5. General Provisions

Firstly: The regulatory body shall harmonize the provisions of this document with its regulatory documents and circulate it to all Its affiliated or related entities, in order to achieve integration and ensure the achievement of the desired goal of preparing these rules.

secondly: The regulatory body is obligated to monitor and document compliance with these general rules on a regular basis.

Third: The entity is committed to complying with these rules and documenting compliance in accordance with the mechanisms and procedures it determines. Regulatory bodies.

Fourth: The entity is committed to informing the regulatory authorities immediately and without delay, and within no more than (72) Hours from the occurrence or discovery of any personal data leak incident, in accordance with the mechanisms and procedures determined by the regulatory authorities.

Fifth: When contracting with other processing entities, the entity is committed to periodically verifying compliance with Other parties shall abide by these rules in accordance with the mechanisms and procedures determined by the regulatory authority, provided that this includes any subsequent contracts concluded by the entity.

Sixth: The Office exercises the roles and functions of regulatory bodies over entities not subject to regulatory bodies. **Seventh:**The regulatory authority has the right to set additional rules for the use of certain special technologies and algorithms. With artificial intelligence after coordination with the office.

Eighth: The regulatory body is committed - after coordination with the office - to preparing the mechanisms and procedures that regulate the process of Handling complaints and objections within a specific time frame and in accordance with the governance model issued by the office.