Resolution No. (2) of 2017

Approving the Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai[1]

The Chairman of the Board of Directors of the Smart Dubai City Office,

After perusal of:

Law No. (11) of 2014 Establishing the Dubai Electronic Security Centre;

Law No. (26) of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai;

Law No. (29) of 2015 Establishing the Smart Dubai City Office; and

Law (2) of 2016 Establishing the Dubai Data Establishment, and

Based on the approval of the Board of Directors of the Smart Dubai City Office in its meeting No. (11) convened on 26 October 2017,

Does hereby issue this Resolution.

Policies Approval

Article (1)

Pursuant to this Resolution, the attached Policies Document, inclusive of the rules, procedures, regulations, forms, and mechanisms regulating the classification, dissemination, exchange, and protection of Data in the Emirate of Dubai, is approved.

©2018 The Supreme Legislation Committee in the Emirate of Dubai

[1]*Every effort has been made to produce an accurate and complete English version of this legislation. However, for the purpose of its interpretation and application, reference must be made to the original Arabic text. In case of conflict, the Arabic text will prevail.*

Supervision of the Implementation of Policies

Article (2)

The Dubai Data Establishment will be responsible for supervising the implementation of the policies referred to in Article (1) of this Resolution.

Publication and Commencement

Article (3)

This Resolution will be published in the Official Gazette and will come into force on the day on which it is published.

Saeed Mohammed Al Tayer

Chairman of the Board of Directors of the Smart Dubai City Office

Issued in Dubai on 26 October 2017

Corresponding to 6 Safar 1439 A.H.

Policies Document on Classification, Dissemination, Exchange, and Protection of Data in the Emirate of Dubai

Chapter One
Definitions, Contents, Scope of Application, and Objectives

Definitions
Article (1)

The following words and expressions, wherever mentioned in this Document, will have the meaning indicated opposite each of them unless the context implies otherwise:

UAE:	The United Arab Emirates.
Emirate:	The Emirate of Dubai.
Government:	The Government of Dubai.
Law:	Law No. (26) of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai.
SDO:	The Smart Dubai City Office.
DDE:	The Dubai Data Establishment.
Federal Government Entity:	Any of the ministries, public agencies and corporations, or similar entities affiliated to the Federal Government.
Local Government Entity:	Any of the Government departments, public agencies and corporations, councils, centres, authorities, or other entities affiliated to the Government, including the authorities supervising Special Development Zones and free zones.
Government Entity:	Any Local Government Entity or Federal Government Entity that has in its possession Data relating to the Emirate.
Private Entity	Any for-profit or non-profit non-governmental legal entity, including sole proprietorships.

Data:	A collection of organised or unorganised information, facts, concepts, instructions, observations, or measurements, in the form of numbers, letters, symbols, images, or any other form, that are collected, produced, or processed by Data Providers. This includes "information" wherever mentioned in this Document.
Dubai Data:	The Data which is in the possession of Data Providers and is related to the Emirate.
Dubai Data Manual:	A document which is approved by the DDE; which includes a set of rules, standards, forms, and procedures regulating the dissemination, exchange, and protection of Dubai Data; and which must be used as a reference by Data Providers.
Electronic Platform:	An electronic system which is composed of hardware, software, networks, storage systems, and a connectivity and communication site; and through which Dubai Data is disseminated and exchanged.
Data Providers:	The Government Entities and Persons determined by the DDE.
Person:	A natural person or a private legal person, including, without limitation, individuals; sole proprietorships; public-benefit establishments; companies; societies; and similar entities.
Open Data:	The Dubai Data which may be disseminated without restrictions or with the relevant minimum restrictions prescribed by the DDE.
Shared Data:	The Dubai Data which is exchanged among Data Providers in accordance with the relevant conditions and rules determined by the DDE.
Confidential Data:	Shared Data whose disclosure to the public or to third parties may cause limited damage to the public interest or to Persons.
Sensitive Data:	Shared Data whose disclosure to the public or exchange by Government Entities on other than a "need-to-know" basis may cause significant damage to the public interest or to Persons.
Secret Data:	Shared Data which is classified as secret and whose disclosure to the public or exchange by Government Entities on other than a "need-to-

	know" basis may cause very serious damage to the public interest, to national security, or to Persons.
Personal Data:	Data that is related to a Person, including personally identifying information, and which may not be available to the public without his consent.
Sensitive Personal Data:	Personal Data that reveals information about or is, directly or indirectly, related to a Person's family; racial, ethnic, or social origin; affiliations; political views; religious or philosophical beliefs; criminal record; membership in unions; health; or personal life.
Private Entity's Data:	Any Data which is related to a Private Entity and which is available to the public and can be used to identify the name, the objectives, and the legal status of that entity.
Private Entity's Sensitive Data:	Any Data which is related to the business of a Private Entity and which is not expected to be made available to the public, including information relating to its officials or employees; revenues or profits; customer lists; or technical know-how, or relating to any of its Intellectual Property Rights.
Data Set:	A collection of organised Data which can be collected, described, and explained; and whose source can be identified.
Data Inventory:	The process of preparing a list of the Data relating to the Emirate that is in the possession of any entity, including any Dubai Data produced or controlled by that entity.
Data Classification Process:	The procedures stipulated in the Dubai Data Manual, including Data Classification Standards, Data format, metadata, and Data quality.
Data Classification Standards:	The standards for classifying Data into Open Data or Shared Data; and for classifying Shared Data into Confidential Data, Sensitive Data, or Secret Data.
Data Sprints:	The sequential ingestion of Data into the Electronic Platform starting with the highest-priority Data.

User:	A Person or Government Entity that benefits from Open Data, and is under an obligation to use it in accordance with the terms and conditions stipulated in the Licence.
Licence:	A document issued by the DDE authorising a User to access Open Data published on the Electronic Platform, in accordance with the relevant conditions and procedures adopted by the DDE and with the terms stipulated in that document.
Access Permission:	An approval issued by a Government Entity authorising a Person to access Shared Data in accordance with the conditions and procedures adopted by that Government Entity or the DDE.
Authorised Person:	Any Person or Government Entity that is authorised by another Government Entity or the DDE to access Confidential Data, Sensitive Data, or Secret Data.
Data Team:	A work team which is formed within a Government Entity and which is comprised of a Data leader, Data administrator, Data expert, Data specialist, and Data steward.
Intellectual Property Rights:	These include patents; rights to inventions; copyright and related rights; trademarks and service marks; trade names and domain names; rights in trade dress; goodwill; the right to sue for passing off or for unfair competition; rights in designs; rights in computer software; rights to use and to protect the confidentiality of confidential information, including know-how and trade secrets; and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for renewals or extensions of and rights to claim priority from such rights, and all similar or equivalent forms of protection which subsist or will subsist, now or in the future, in any part of the world.
Primary Registers:	The electronic or paper-based registers which are determined, organised, and classified by the DDE to ensure that each of them includes a specific and consistent type of Dubai Data.

Working Day:	Any of the official working days of a Government Entity as per the working hours it adopts.

Contents

Article (2)

This Document contains the following policies for Data dissemination and exchange:

1. Policy for Data Classification;
2. Policy for Protection of Data and Policy for Intellectual Property Rights;
3. Policy for the Use and Reuse of Dubai Data; and
4. Policy for Technical Standards.

Scope of Application

Article (3)

a. The provisions of this Document will apply to:

    1. Federal Government Entities which have in their possession any Data relating to the Emirate;

    2. Local Government Entities; and

    3. Persons who produce, own, disseminate, or exchange Data relating to the Emirate and who are determined by the DDE, including those existing in Special Development Zones and free zones, such as the Dubai International Financial Centre.

b. The entities referred to in paragraph (a) of this Article must implement this Document in accordance with the scheduled phases prescribed by the DDE.

Objectives

Article (4)

In addition to the objectives stipulated in the Law, this Document aims to:

1. enhance and support the Emirate's efforts in realising its Smart Transformation vision;

2. regulate the dissemination, exchange, use, reuse, and disposal of Open Data and Shared Data;

3. facilitate access to Open Data and Shared Data;

4. achieve integration among Government Entities; and enhance the efficiency of, and synergy among, their services through improving quality, speeding delivery, streamlining procedures for customers, and reducing operating costs;

5. protect the privacy of individuals' Data; the confidentiality of business Data; and their Intellectual Property Rights;

6. minimise the duplication of the Data maintained by Government Entities;

7. support the decision-making process at Government Entities by providing them with accurate Data in order to enable them to develop their policies, to implement their strategic plans and initiatives efficiently and effectively, and to anticipate the future;

8. enhance transparency and establish the rules of governance through division of roles and responsibilities between the DDE and Government Entities;

9. determining the rights and obligations of Persons dealing with Personal Data and Private Entities' Data; and

10. set clear procedures for filing grievances against the decisions issued by the DDE or Government Entities in respect of Data dissemination and exchange.

Chapter Two

Preliminary Provisions

Data Inventory

Article (5)

All Government Entities must conduct a Data Inventory pursuant to the relevant procedures prescribed by the Dubai Data Manual, in preparation for Data classification, dissemination, and exchange in accordance with the provisions hereof.

Data Dissemination and Exchange Priority

Article (6)

a. A Government Entity must ensure that Data with high-priority is disseminated and exchanged, particularly:

   1. the Primary Registers or secondary registers that the Government Entity maintains as required by the DDE;

   2. the Data that is disseminated and exchanged for purposes of electronic and smart services;

   3. the Data that is designated by the DDE as high-priority Data given the need for it to implement strategic Government initiatives; achieve the Smart Transformation; or follow up performance indicators; and

   4. the Data that is requested by more than one Government Entity in the Emirate.

b. A Government Entity must implement this Document in accordance with priority-based scheduled phases. This implementation must be done by:

   1. developing, in accordance with the processes set out in the Dubai Data Manual, its own entity-level action plan, setting out the steps it will take to progressively disseminate and exchange its Data through a series of Data Sprints, in accordance with the timetable prescribed by the DDE;

2. conducting a Data Inventory which, in its initial version, lists all high-priority Data Sets of the Government Entity and which will then be expanded based on User feedback to cover all Data Sets managed by that Government Entity; and

3. coordinating with the DDE to approve the high-priority Data to be included in the initial Data Sprints.

c. The DDE must support Government Entities by:

1. setting the timetable for ingesting Data Sprints into the Electronic Platform;

2. providing detailed guidance to Government Entities on how to satisfy the requirements and comply with the Data Inventory and prioritisation criteria in accordance with the Dubai Data Manual;

3. reviewing the Data Inventories conducted by Government Entities to ensure that initial versions fully cover all high-priority Data;

4. approving the high-priority Data for purposes of dissemination or exchange in order to ingest it as part of Data Sprints; and

5. following up Government Entities' implementation of their approved Data dissemination and exchange action plans.

Data Classification Prior to Dissemination or Exchange

Article (7)

A Government Entity must classify Dubai Data which it has in its possession, including any Dubai Data which it produces or controls, as either Open Data or Shared Data in accordance with this Document and using the Data Classification Process set out in the Dubai Data Manual, prior to the dissemination or exchange of that Dubai Data.

Dissemination of Open Data and Exchange of Shared Data

Article (8)

a. A Government Entity which has a set of Open Data or Shared Data must disseminate or exchange it through the Electronic Platform in accordance with the Law, this Document, the Dubai Data Manual, and the terms of the Licence and Access Permissions, to enable any User or Authorised Person to access this Data.

b. The DDE may exempt a Government Entity, upon its request and for a valid reason, from the requirement to disseminate its Open Data or exchange its Shared Data through the Electronic Platform.

c. A Government Entity is prohibited from disseminating, exchanging, or sharing Secret Data through the Electronic Platform.

Using the Electronic Platform

Article (9)

a. Unless otherwise stipulated in this Document, all Government Entities must disseminate Open Data and exchange Shared Data through the Electronic Platform.

b. The DDE must ensure that Open Data is made available to the public through the Electronic Platform.

c. Government Entities must refer, on their websites, to the Open Data available on the Electronic Platform and direct Users to access it using an electronic link.

d. Government Entities must coordinate with the DDE on all matters related to ingesting Data Sprints into the Electronic Platform and updating the same.

e. The DDE will guarantee Government Entities that their Shared Data available on the Electronic Platform is exclusively accessible to Authorised Persons.

Data Team

Article (10)

A Local Government Entity must form a Data Team in accordance with the standards and rules prescribed by the Dubai Data Manual.

Chapter Three

Roles, Responsibilities, and Obligations

Roles of Local Government Entities or Federal Government Entities

Article (11)

In addition to the obligations stipulated in Article (11) of the Law, a Government Entity must:

1. conduct an inventory of its Data and prioritise it for dissemination and exchange purposes in accordance with Articles (5) and (6) of this Document;
2. classify the Dubai Data which it produces or controls, as either Open Data or Shared Data, using the Data Classification Process prescribed by Chapter (4) of this Document;
3. disseminate its Open Data through the Electronic Platform in accordance with the terms of the Licence;
4. exchange its Shared Data in accordance with the relevant Access Permissions;
5. use the Electronic Platform for Data dissemination and exchange;
6. form a Data Team in accordance with the rules of governance stipulated in this Document;
7. protect Dubai Data and its Intellectual Property Rights, and comply with information security requirements in accordance with this Document;
8. cooperate with the DDE on determining the additional costs related to Open Data and developing value-added services in accordance with this Document;

9. cooperate and coordinate, in respect of Dubai Data, with the concerned security bodies and centres in the UAE, in accordance with this Document;

10. submit reports to the DDE on the Government Entity's compliance with this Document and with the Dubai Data Manual; and

11. follow the complaints procedures stipulated in this Document.

Role of the DDE

Article (12)

In addition to the functions assigned to it under the Law, the DDE will have the duties and powers to:

1. supervise the implementation of the Dubai Data Manual and this Document;

2. provide access to the Open Data published on the Electronic Platform;

3. ensure that the Electronic Platform is exclusively used by the Persons authorised to access the Data published thereon pursuant to the relevant Access Permissions;

4. develop, and sell to Users, value-added Data services, in cooperation with Government Entities;

5. support Government Entities in conducting Data Inventories and prioritising their Data for dissemination and exchange purposes;

6. provide detailed guidance to Government Entities within the Dubai Data Manual on how to comply with the requirements of this Document, and publish it on its website;

7. exempt any Government Entity from compliance with certain provisions of this Document;

8. resolve any dispute arising from a Government Entity's refusal to share its Data with another Government Entity;

9. take the necessary measures regarding acts of non-compliance by Government Entities or Persons with the Law, with this Document, or with the policies and regulations adopted by the DDE; and

10. comply with the procedures for investigations and grievances related to Dubai Data.

Obligations of Users and Authorised Persons

Article (13)

A User or Authorised Person must:

1. use Open Data in accordance with the terms of the Licence;

2. use and exchange Shared Data in accordance with the relevant Access Permissions and for the authorised purposes; and

3. in using Open Data and Shared Data, comply with the provisions of the Data Protection Policy and Intellectual Property Rights Policy.

Chapter Four

Data Classification Policy

Data Classification Process

Article (14)

Government Entities must classify its Data in accordance with the provisions of this Document and the Dubai Data Manual.

Open Data Classification

Article (15)

a. A Government Entity will classify a Data Set as Open Data where its dissemination is in the public interest, provided that:

    1. its dissemination does not conflict with the legislation or policies in force in the Emirate;

    2. it does not compromise the safety of individuals or society;

    3. it does not result in disclosure or misuse of any Personal Data, Private Entities' Data, or Private Entities' Sensitive Data;

4. it does not infringe any Intellectual Property Rights; and

5. it does not adversely affect security and administration of justice.

b. All Dubai Data that is not classified as Open Data will be deemed Shared Data.

Shared Data Classification

Article (16)

a. Shared Data will be classified into the following sub-categories:

1. Confidential Data;

2. Sensitive Data; and

3. Secret Data.

b. For purposes of Shared Data Classification into the sub-categories referred to in paragraph (a) of this Article, Government Entities must comply with the provisions of this Document.

Confidential Data Classification Criteria

Article (17)

Shared Data will be deemed Confidential Data where its disclosure to the public or third parties may cause limited damage to the public interest or to Persons. This includes:

1. disclosing Personal Data (excluding Sensitive Personal Data) for a purpose other than that for which it is collected;

2. adversely affecting the ability of a Federal Government Entity or a Local Government Entity to perform its duties;

3. causing limited damage to the assets of a Person or causing him a limited financial loss;

4. causing a limited negative impact on the reputation of a Person or a Private Entity;

5. adversely affecting a Private Entity by limiting its competitiveness; or

6. adversely affecting public safety or justice.

Sensitive Data Classification Criteria

Article (18)

Shared Data will be deemed Sensitive Data where its disclosure to the public may cause significant damage to public interest or to Persons. This includes:

1. disclosing Sensitive Personal Data, such as information on a person's health condition, or Private Entities' Sensitive Data, for a purpose other than that for which the Data is collected;
2. directly threatening a Person's life, freedom, or safety;
3. infringing any Intellectual Property Rights without the right holder's permission;
4. causing significant damage to the assets of a Government Entity or a Person, or causing that Person significant financial loss;
5. causing a negative impact on the reputation of a Person or Government Entity;
6. causing significant damage to a Person or Private Entity that may lead to loss of cognitive and intellectual advantages or incurring financial losses;
7. causing significant damage to the ability of a Federal Government Entity or a Local Government Entity to perform its duties;
8. causing significant damage to the operational effectiveness of highly valuable security operations;
9. causing significant damage to diplomatic relations with any country or international organisation;
10. causing significant damage to the safety, security, or prosperity of the UAE; any emirate of the UAE; or any other country, by affecting its commercial, economic, or financial interests;
11. causing significant damage to the security of critical national infrastructure;

12. causing significant damage to the operational effectiveness of the police authorities or military forces of the UAE in a way that causes them to encounter, in the course of performing their duties, the following situations:

    1. inability to use their present or future capabilities;
    2. loss of life;
    3. damage to their facilities, rendering them unusable; or
    4. a negative impact on the administration of justice, including the ability to investigate crimes or prosecute perpetrators.

Secret Data Classification Criteria

Article (19)

Shared Data will be deemed Secret Data where its disclosure to the public or exchange within the Government on other than a "need-to-know" basis is illegal and may cause very serious damage to the public interest, to national security, or to Persons. This includes:

1. disclosing the Personal Data, Sensitive Personal Data, Private Entities' Data, or Private Entities' Sensitive Data of a Person mentioned on the lists prepared for this purpose;
2. infringing any Intellectual Property Rights which belong to a Person mentioned on the lists prepared for this purpose, even where the use of such rights has a lawful and fair basis;
3. causing heavy loss of life;
4. causing a significant or noticeable negative impact on the public interest or national security of the Emirate, or of any other emirate of the UAE;
5. compromising the domestic stability of the Emirate, or of any other emirate of the UAE;
6. causing disruption and tension in international relations;
7. causing very serious damage to the capabilities or security of the UAE or its allied forces, leading to their inability to perform military duties;
8. causing very serious damage to relations with friendly nations or recognised international organisations;

9. causing very serious damage to major security or intelligence operations;
10. causing long-term damage to the economy of the Emirate, or of any other emirate of the UAE;
11. causing very serious damage to the ability of any of the Local Government Entities to perform its duties or to its assets, or adversely affecting its reputation leading to loss of public confidence in that Local Government Entity;
12. causing very serious damage to a Private Entity that has a vital and strategic role in the national economy, resulting in heavy financial losses, bankruptcy, or loss of its leading role;
13. seriously compromising the safety and lives of certain personnel of the police, security, or military authorities; or of witnesses in critical court cases; and
14. adversely affecting security and the administration of justice, or obstructing investigations into serious crimes or prosecution of perpetrators.

Shared Data Access Permissions

Article (20)

a. No Person may access Shared Data without first obtaining an Access Permission.

b. A Government Entity must specify, in accordance with the provisions of this Document, the Government Entities and Private Entities that are authorised to access its Shared Data.

c. Access Permissions will be issued to entities other than those referred to in paragraph (b) of this Article in accordance with the following procedures:

    5. A request for Access Permission, stating the reasons and justifications for this request, will be submitted through the Electronic Platform to the Government Entity responsible for the Shared Data Set.
    6. The Government Entity must approve or reject the request within fifteen (15) Working Days from the date of its submission, and its decision must be reasoned where the request is rejected.
    7. The DDE must take the actions required for granting Access Permission where the relevant Government Entity fails to respond to the Access Permission request within the period referred to in paragraph (c)(2) of this Article.

d. The DDE must verify that the Government Entity complies, in the course of exchanging Shared Data, with this Document and the Dubai Data Manual.

e. The DDE must resolve any dispute that may arise from the Government Entity's rejection to share its Data with another entity. The DDE's decision in respect of the dispute will be final and binding.

f. Subject to liability, an Authorised Person must comply with the terms of the Access Permission and with the legislation in force in the Emirate.

Chapter Five

Data Protection Policy and Intellectual Property Rights Policy

Data Protection

Article (21)

a. The entities and Persons governed by this Document must not disclose, or otherwise classify as Open Data and disseminate, any Personal Data, Private Entities' Data, or Private Entities' Sensitive Data.

b. In the course of implementing the Data Classification Process, a Data Team must identify Personal Data, Private Entities' Data, and Private Entities' Sensitive Data which may not be included in an Open Data Set. In any event, Dubai Data may not be classified as Open Data until all restricted Data, as per the classification, is removed.

Protection of Intellectual Property Rights

Article (22)

Dubai Data which is encumbered by third party Intellectual Property Rights may not be disseminated as Open Data or exchanged as Shared Data without the consent of the owner of these rights.

Obtaining Consent

Article (23)

A Government Entity must:

1. seek the consent of individuals and Private Entities to use, store, process, and exchange with other Government Entities in the Emirate their Personal Data, Private Entities' Data, or Private Entities' Sensitive Data to enable any Government Entity to provide services to its customers without the need to request the same Data again;
2. obtain the consent of the relevant Intellectual Property Rights holder, where it is commercially viable for both the rights holder and the Government Entity, to use or reproduce protected Data for the purpose of the Government Entity providing its services to its customers;
3. provide options for individuals and Private Entities to amend their Data or revoke their consent on exchanging their Data among Government Entities;
4. adhere to the following principles, when handling Personal Data, Private Entities' Data, or Private Entities' Sensitive Data; or granting Access Permissions related thereto:
    a. Transparency: by informing individuals and Private Entities of which Government Entity will collect their Personal Data or private Data.
    b. Purpose: by using the collected Data for specific and explicitly stated purposes.
    c. Proportionality: by ensuring that the type of Data collected is the minimum required to achieve the purpose for which it is collected.

Information Security Regulation

Article (24)

In implementing this Document and the information security regulations and standards issued in pursuance of the Law, Local Government Entities must comply with the Information Security Regulation issued by the Dubai Electronic Security Centre.

Chapter Six

Dubai Data Use and Reuse Policy

Open Data Licence

Article (25)

In accessing Open Data through the Electronic Platform, Users and Private Entities must comply with the terms and conditions of the Licence.

Shared Data Exchange

Article (26)

In exchanging Shared Data, a Government Entity must:

1. modify and reclassify Shared Data as Open Data, in the event of making it available to the public, in accordance with this Document and with the Dubai Data Manual;
2. exchange Shared Data in accordance with the relevant Access Permissions;
3. make Confidential Data available at all times, through the Electronic Platform, to other Local Government Entities and to any other Authorised Persons;
4. exchange any Sensitive Data, included in the Shared Data, with Authorised Persons on a "need-to-know" basis only; and
5. exchange any Sensitive Data by means other than the Electronic Platform, subject to obtaining the prior relevant approval of the DDE.

Disposal of Dubai Data

Article (27)

a. Dubai Data is a Government asset and may be disposed of as follows:
    1. Open Data may be sold subject to the following conditions:
        a. Open Data must be sold only under exceptional circumstances;

b. the relevant Government Entity or DDE must have been incurring additional costs in collecting, processing, or providing Open Data;

c. the sale of Open Data must be made exclusively through the Electronic Platform;

d. the sale price of Open Data must be determined by the DDE in coordination with the relevant Government Entity; and

e. the methods of determining and collecting the sale price of Open Data must be appropriate in view of the additional costs incurred by the relevant Government Entity or DDE.

2. The DDE may sell value-added Data services subject to the following conditions:

a. the sale of the services must be aimed at achieving the public interest and the Smart Transformation goals;

b. value-added Data may only be made available through the Electronic Platform;

c. re-use of the Open Data, used as the basis for developing the value-added Data services, on a competitive basis by Private Entities must be fostered;

d. the value-added Data services must be made available to all Users on a fair, reasonable, and non-discriminatory basis, and the DDE may not launch the value-added Data services until the Open Data on which it is based is also published on the Electronic Platform; and

e. the sale price of the value-added Data services must be determined in a way that enables recovery of as much as possible of the total costs of providing these services and in line with the market price.

b. A Government Entity may apply for an exemption from compliance with the requirements prescribed in paragraph (a)(1) of this Article, provided that the reasons and justifications for exemption are stated in the application. In any event, the Local Government Entity must comply with these requirements until the application for exemption is determined.

c. A Government Entity that has a contract or an obligation for the provision or sale of Data to another party, or sharing Data with that party, in contravention of paragraph (a) of this Article must:

1. terminate the contract or obligation as soon as possible, provided that this termination does not result in incurring any financial liabilities;
2. not renew the contract upon its expiry; and
3. not enter into new contracts without first obtaining the approval of the DDE.

Chapter Seven
Technical Standards Policy
Article (28)

a. The DDE must publish on its website the Dubai Data Manual, which comprises the governance frameworks and business processes related to Data dissemination and exchange, including Data technical standards.

b. The DDE must specify which elements of the standards set out in the Dubai Data Manual, specifically the technical standards, are mandatory and which elements are only recommended.

Chapter Eight
Final Provisions

Public Interest
Article (29)

The DDE, and the entities and Persons governed by this Document, must take the exigencies of public interest and public security into consideration, seeking in particular to:

1. promote the concept of accountability and transparency;
2. protect public health and safety;

3. protect consumers;

4. support economic sectors;

5. foster the provision of better Government services;

6. protect public security;

7. strengthen international relations, including political and economic relations with foreign governments and international organisations;

8. foster legislative stability, proper implementation of legislation, and compliance with the principles of governance;

9. support and protect vital economic, academic, and technology sectors to achieve stability, safety, and welfare;

10. preserve national heritage and culture;

11. prevent crime and protect the safety of individuals; and

12. maintain the UAE infrastructure, strategic, and vital services.

Cooperation and Coordination with Security Bodies

Article (30)

Government Entities must provide support and assistance to the concerned security authorities in performing their work and duties, including by providing the Data that they request with a view to serving the public interest, national interest, and public security.

Reports

Article (31)

Local Government Entities must submit to the DDE periodic reports on their performance based on the relevant performance criteria approved by the DDE. The reporting process, reporting frequency, and reports' contents must be determined by the Dubai Data Manual.

Complaint Procedures

Article (32)

a. Any Person may file a complaint in relation to the implementation of this Document or the Dubai Data Manual.

b. Complaints must be based on any of the following grounds:

   1. breach of the provisions of the Law or this Document, or any of the policies issued in pursuance thereof;

   2. failure by the DDE or a Local Government Entity to comply with the rules related to disposal or classification of Data;

   3. an Open Data Set containing Personal Data, Private Entities' Data, Private Entities' Sensitive Data, or infringing any Intellectual Property Rights; or

   4. breach of Licence or Access Permission by a User or an Authorised Person.

c. The procedures for receiving and determining complaints will be governed by the Dubai Government's Unified Customer Complaints Guide.

d. Where the complainant is not satisfied with the decision of the Local Government Entity in respect of his complaint, he may file an appeal with the DDE. The DDE may, on its own initiative, investigate any act of non-compliance, by any Person or entity, with the provisions of this Document or the Dubai Data Manual.

e. All Local Government Entities must, within the time frame prescribed by the DDE, provide the DDE with any information related to the investigations it is conducting.

f. The DDE will determine a complaint submitted to it within sixty (60) Working Days from the date of receipt of the complaint. The DDE will take the necessary measures in respect of any breach of this Document or the Dubai Data Manual. In any event, the DDE will notify the complainant and the SDO of the relevant findings.

Actions and Measures

Article (33)

a. The DDE must take the necessary actions and measures upon discovering that a Person has committed any violation of the provisions of the Law, this Document, the Licence, or the relevant Access Permission.

b. The DDE will notify the violating Person or Government Entity of the violation and the remedial action that must be taken within the time frame that the DDE prescribes.

c. Where the violating Person or Government Entity fails to take the above-mentioned remedial action, the DDE will take the following measures:

   1. order the violating Person or Local Government Entity to remedy the violation or permanently desist from committing the violation;

   2. issue a warning to the violating User or Authorised Person;

   3. revoke the violator's Access Permission; and

   4. submit a report to the Executive Council of the Emirate of Dubai on the violations committed by Government Entities.

Grievances

Article (34)

a. Any affected party may submit a written grievance to the CEO of the DDE against the decisions, procedures, and measures taken against him in accordance with the provisions of this Document and the resolutions issued in pursuance hereof, within fifteen (15) Working Days from the date of being notified of the contested decision, procedure, or measure. The grievance will be determined, within thirty (30) Working Days from the date of its submission, by a committee formed by the CEO for this purpose, and the decision issued by the committee on the grievance will be final.

b. The terms of reference of the committee referred to in paragraph (a) of this Article, and the procedures for filing grievances, will be determined pursuant to a resolution issued by the CEO of the DDE in this respect.

Compliance

Article (35)

All Local Government Entities must modify their Data in accordance with the provisions of this Document within one (1) year from the effective date hereof.

Issuing Implementing Resolutions

Article (36)

The CEO of the DDE will issue the resolutions required for the implementation of the provisions of this Document.