Federal Decree-Law No. 45/2021
On the Protection of Personal Data

Type	Law
Issued on	20 Sep 2021 (corresponding to 13 Safar 1443 H)
Nature	Decree-Law
Jurisdiction	United Arab Emirates

We, Khalifa bin Zayed Al Nahyan, President of the United Arab Emirates,

Having perused:

The Constitution;

Federal Law No. 1/1972 on the Competencies of the Ministries and Powers of the Ministers, as amended;

Federal Decree-Law No. 3/2003 Regulating the Telecommunications Sector, as amended;

Federal Law No. 6/2010 on Credit Information, as amended;

Federal Law No. 14/2016 on Violations and Administrative Penalties in the Federal Government;

Federal Law No. 2/2019 on the Use of Information and Communication Technology (ICT) in Health Fields;

Federal Decree-Law No. 14/2018 on the Central Bank and Organisation of Financial Institutions and Activities, as amended

Federal Decree-Law No. 44/2021 Establishing the UAE Data Office; and

Based on the proposal of the Minister of Cabinet Affairs and the approval of the Cabinet,

have issued the following Decree Law:

Article 1 - Definitions

In applying the provisions of this Decree Law, the following words and expressions shall have the meanings assigned to each, unless the context otherwise requires:

State:	The United Arab Emirates.
Office:	The UAE Data Office established by virtue of Federal Decree-Law No. 44/2021 referred to above.
Data:	An organized or unorganized set of data, facts, concepts, instructions, views, or measurements, in the form of numbers, letters, words, symbols, images, videos, signs, sounds, maps, or any other form, that is interpreted, exchanged or processed by humans or computers, which also includes information wherever it appears herein.
Personal Data:	Any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking data, using identifiers such as name, voice, picture, identification number, online identifier, geographic location, or one or more special features that express the physical, psychological, economic, cultural or social identity of such person. It also includes Sensitive Personal Data and Biometric Data.
Sensitive Personal Data:	Any data that directly or indirectly reveals a natural person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data, or any data related to the health of such person, such as his/her physical, psychological, mental, genetic or sexual condition, including information related to health care services provided thereto that reveals his/her health status.
Biometric Data:	Personal Data resulting from Processing, using a specific technique, relating to the physical, physiological or behavioral characteristics of a Data Subject, which allows or confirms the unique identification of the Data Subject, such as facial images or dactyloscopic data.
Data Subject:	The natural person who is the subject of the Personal Data.
Establishment:	Any company or sole proprietorship established inside or outside the State, including companies which the federal or local government partially or wholly owns or has a shareholding therein.
Controller:	An establishment or natural person who has Personal Data and who, given the nature of his/her activity, specifies the method, criteria and purpose of Processing such Personal Data, whether individually or jointly with other persons or establishments.
Processor:	An establishment or natural person who processes Personal Data on behalf of the Controller, as directed and instructed by the Controller.
Data Protection Officer:	Any natural or legal person appointed by the Controller or Processor to undertake the responsibilities of ascertaining the compliance of his/her entity with the controls, conditions, procedures and rules for Processing and protecting Personal Data stipulated herein, and ascertaining the integrity of its systems and procedures in order to ensure compliance with the provisions hereof.
Processing:	Any operation or set of operations which is performed on Personal Data using any electronic means, including Processing and other means. This process includes collection, storage, recording, organization, adaptation, alteration, circulation, modification, retrieval, exchange, sharing, use, or classification or disclosure of Personal Data by transmission, dissemination or distribution, or otherwise making it available, or aligning, combining, restricting, blocking, erasing or destroying Personal Data or creating models therefor.

Automated Processing:	Processing that is carried out using an electronic program or system that is automatically operated, either completely independently without any human intervention, or partially independently with limited human supervision and intervention.
Personal Data Security:	A set of technical and organizational measures, procedures and operations, specified according to the provisions hereof, aimed at protecting the privacy, secrecy, safety, unity, integrity and availability of Personal Data.
Pseudonymization:	The Processing of Personal Data in such a way that the data, after completion of Processing, can no longer be linked and attributed to the Data Subject without the use of additional information, as long as such additional information is kept separately and safely and subject to the technical and organizational measures and procedures, specified according to the provisions hereof, to ensure non-attribution of Personal Data to an identified or identifiable natural person.
Anonymization:	The Processing of Personal Data in such a way that anonymizes the Data Subject's identity so that such data can no longer be linked and attributed to the Data Subject and the Data Subject can no longer be identified in any way whatsoever.
Data Breach:	A breach of information security and Personal Data by illegal or unauthorized access, including copying, sending, distributing, exchanging, transmitting, circulating or Processing data in a way that leads to disclosure thereof to third parties, or damage or alteration thereof during the processes of storage, transmission and Processing.
Profiling:	A form of Automated Processing consisting of the use of Personal Data to evaluate certain personal aspects relating to a Data Subject, including to analyze or predict aspects concerning his/her performance, economic situation, health, personal preferences, interests, behavior, location, movements or reliability.
Cross-Border Processing:	Dissemination, use, display, transmission, receipt, retrieval, sharing or Processing of Personal Data outside the territory of the State.
Consent:	The consent given by a Data Subject to authorize third parties to process his/her Personal Data, provided that such consent is a specific, informed and unambiguous indication of the Data Subject's agreement to the Processing of his/her Personal Data, by a statement or by a clear affirmative action.

Article 2 - Applicability of the Decree Law

1. The provisions of this Decree Law shall apply to the Processing of Personal Data, whether totally or partially, through automatically operated electronic systems or other means, by:
    - a. any Data Subject who resides or has a place of business in the State.
    - b. any Controller or Processor located in the State who carries out the activities of Processing Personal Data of Data Subjects inside or outside the State.
    - c. any Controller or Processor located outside the State who carries out the activities of Processing Personal Data of Data Subjects inside the State.
2. The provisions of this Decree Law shall not apply to the following:
    - a. government data.
    - b. government authorities that control or process Personal Data.
    - c. Personal Data held with security and judicial authorities.
    - d. a Data Subject who processes his/her data for personal purposes.
    - e. health personal data that is subject to legislation regulating the protection and Processing thereof.
    - f. banking and credit personal data and information that is subject to legislation regulating the protection and Processing thereof.
    - g. companies and institutions located in the free zones of the State and are subject to special legislation on Personal Data Protection.

Article 3 - Office's Power of Exemption

Without prejudice to any other competencies established for the Office under any other legislation, the Office may exempt those Establishments that do not process a large amount of Personal Data from all or some of the requirements and conditions of the provisions of Personal Data Protection stipulated herein, in accordance with the standards and controls set by the Executive Regulations of this Decree Law.

Article 4 - Cases of Processing Personal Data without the Data Subject's Consent

It is prohibited to process Personal Data without the consent of the Data Subject. However, the following cases, in which Processing is considered lawful, are excluded from such prohibition:

1. if the Processing is necessary to protect the public interest.
2. if the Processing is for Personal Data that has become available and known to the public by an act of the Data Subject.
3. if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures.
4. if the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the State.
5. if the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the State.
6. if the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the State.
7. if the Processing is necessary to protect the interests of the Data Subject.
8. if the Processing is necessary for the Controller or Data Subject to fulfill his/her obligations and exercise his/her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws.
9. if the Processing is necessary to perform a contract to which the Data Subject is a party or to take, at the request of the Data Subject, procedures for concluding, amending or terminating a contract.
10. if the Processing is necessary to fulfill obligations imposed by other laws of the State on Controllers.
11. any other cases set by the Executive Regulations of this Decree Law.

Article 5 - Personal Data Processing Controls

Personal Data shall be processed according to the following controls:

1. Processing must be made in a fair, transparent and lawful manner.
2. Personal Data must be collected for a specific and clear purpose, and may not be processed at any subsequent time in a manner incompatible with that purpose. However, Personal Data may be processed if the purpose of Processing is similar or close to the purpose for which such data is collected.
3. Personal Data must be sufficient for and limited to the purpose for which the Processing is made.
4. Personal Data must be accurate and correct and must be updated whenever necessary.
5. Appropriate measures and procedures must be in place to ensure erasure or correction of incorrect Personal Data.
6. Personal Data must be kept securely and protected from any breach, infringement, or illegal or unauthorized Processing by establishing and applying appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard.
7. Personal Data may not be kept after fulfilling the purpose of Processing thereof. It may only be kept in the event that the identity of the Data Subject is anonymized using the “Anonymization” feature.
8. Any other controls set by the Executive Regulations of this Decree Law.

Article 6 - Conditions for Consent to Data Processing

1. In order to accept the Consent of the Data Subject to Processing, the following conditions must be met:
    - A. The Controller must be able to prove the Consent of the Data Subject to process his/her Personal Data in the event that the Processing is based on such Consent.
    - B. The Consent must be given in a clear, simple, unambiguous and easily accessible manner, whether in writing or electronic form.
    - C. The Consent must indicate the right of the Data Subject to withdraw it and that such withdrawal must be easily made.
2. The Data Subject may, at any time, withdraw his/her Consent to the Processing of his/her Personal Data. Such withdrawal shall not affect the legality and lawfulness of the Processing made based on the Consent given prior to the withdrawal.

Article 7 - General Obligations of the Controller

The Controller shall:

1. take the appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure Personal Data, in order to maintain its confidentiality and privacy and to ensure that it is not infringed, damaged, altered or tampered with, taking into account the nature, scope and purposes of Processing and the potential risks to the confidentiality and privacy of the Personal Data of the Data Subject.
2. apply the appropriate measures, both when defining the means of Processing or during the Processing itself, in order to comply with the provisions of this Decree Law, including the controls stipulated in Article (5) thereof. Such measures include Pseudonymization.
3. apply the appropriate technical and organizational measures with respect to default settings to ensure that the Processing of Personal Data is limited to its intended purpose. This obligation applies to the amount and type of Personal Data collected, the type of Processing to be made thereon, and the period of storage and accessibility of such data.
4. maintain a special record of Personal Data which must include the data of the Controller and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Controller provides this record to the Office whenever requested to do so.
5. appoint a Processor who provides sufficient guarantees to apply technical and organizational measures in a manner that ensures that the Processing meets the Processing requirements, rules and controls stipulated in this Decree Law, the Executive Regulations thereof and decisions issued in implementation thereof.
6. provide the Office, based on a decision from the competent judicial authority, with any information requested thereby in exercise of its competencies stipulated in this Decree Law and the Executive Regulations thereof.
7. fulfill any other obligations set by the Executive Regulations of this Decree Law.

Article 8 - General Obligations of the Processor

The Processor shall:

1. make and carry out the Processing in accordance with the instructions of the Controller and the contracts and agreements concluded between them that specify in particular the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects.
2. apply the appropriate technical and organizational measures and procedures to protect Personal Data at the design stage, both when defining the means of Processing or during the Processing itself, taking into consideration the cost of applying such measures and procedures and the nature, scope and purposes of the Processing.
3. make the Processing according to the purpose and period set therefor, and notify the Controller if the Processing exceeds the set period, in order to extend such period or issue the appropriate directions.
4. erase the data after expiry of the Processing period or hand it over to the Controller.
5. not to take any action that would disclose the Personal Data or the results of Processing, except in cases permitted by law.
6. protect and secure the Processing operation and secure the media and electronic devices used in the Processing and the Personal Data stored therein.
7. maintain a special record of Personal Data processed on behalf of the Controller, which must include the data of the Controller, Processor and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Processor provides this record to the Office whenever requested to do so.
8. provide all means to prove abidance thereby to the provisions of this Decree Law, at the request of the Controller or Office.
9. make and carry out the Processing in accordance with the rules, requirements and controls set by this Decree Law and the Executive Regulations thereof, or as instructed by the Office.
10. If the Processing involves more than one Processor, the Processing must be made in accordance with a contract or written agreement whereby their obligations, responsibilities and roles related to the Processing are clearly defined, otherwise they shall be held jointly liable for the obligations and responsibilities stipulated in this Decree Law and the Executive Regulations thereof.
11. The Executive Regulations of this Decree Law shall set the procedures, controls, conditions, and technical and standard criteria related to such obligations.

Article 9 - Reporting a Personal Data Breach

1. In addition to the obligations of the Controller stipulated herein, the Controller shall, immediately upon becoming aware of any infringement or breach of the Personal Data of the Data Subject that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the Office within such period and in accordance with such procedures and conditions as set by the Executive Regulations of this Decree Law. Such reporting shall be accompanied by the following data and documents:
    - a. the nature, form, causes, approximate number and records of the infringement or breach.
    - b. the data of the Data Protection Officer appointed thereby.
    - c. the potential and expected effects of the infringement or breach.
    - d. the procedures and measures taken thereby and proposed to be applied to address this infringement or breach and reduce its negative effects.
    - e. documentation of the infringement or breach and the corrective actions taken thereby.
    - f. any other requirements by the Office.
2. In all cases, the Controller must notify the Data Subject in the event that the infringement or breach would prejudice the privacy, confidentiality and security of his/her Personal Data and advise him/her of the procedures taken thereby, within such period and in accordance with such procedures and conditions as set by the Executive Regulations of this Decree Law.
3. The Processor shall, immediately upon becoming aware of any infringement or breach of the Personal Data of the Data Subject, notify the Controller of such infringement or breach in order for the Controller, in turn, to report it to the Office in accordance with Item (1) of this Article.
4. After receiving the report from the Controller, the Office shall verify the causes of the infringement and breach to ascertain the integrity of the security measures taken, and shall impose the administrative penalties stated in Article (26) of this Decree Law if it is proven that the Controller or Processor violates the provisions of this Decree Law and decisions issued in implementation thereof.

Article 10 - Appointment of Data Protection Officer

1. The Controller and Processor shall appoint a Data Protection Officer who has sufficient skills and knowledge of Personal Data Protection, in any of the following cases:
    - a. if the Processing would cause a high-level risk to the confidentiality and privacy of the Personal Data of the Data Subject as a result of adopting technologies that are new or associated with the amount of data.
    - b. if the Processing will involve a systematic and comprehensive assessment of Sensitive Personal Data, including Profiling and Automated Processing.
    - c. if the Processing will be made on a large amount of Sensitive Personal Data.
2. The Data Protection Officer may be employed or authorized by the Controller or Processor, whether inside or outside the State.
3. The Controller or Processor shall specify the contact address of the Data Protection Officer and notify the Office thereof.
4. The Executive Regulations of this Decree Law shall specify the types of technologies and criteria for determining the amount of data required in accordance with this Article.

Article 11 - Responsibilities of the Data Protection Officer

1. The Data Protection Officer shall be responsible for ascertaining compliance by the Controller or Processor with the provisions of this Decree Law, the Executive Regulations thereof, and the instructions issued by the Office. The Data Protection Officer shall, in particular, undertake the following duties and powers:
    - a. verifying the quality and validity of the procedures adopted by both the Controller and Processor.
    - b. receiving requests and complaints related to Personal Data in accordance with the provisions of this Decree Law and the Executive Regulations thereof.
    - c. providing technical advice related to the procedures of periodic evaluation and examination of Personal Data Protection systems and intrusion prevention systems of the Controller and Processor, documenting the results of such evaluation, and providing appropriate recommendations in this regard, including risk assessment procedures.
    - d. acting as a liaison between the Controller or Processor, as the case may be, and the Office regarding their implementation of the provisions of Personal Data Processing stipulated herein.
    - e. any other duties or powers specified under the Executive Regulations of this Decree Law.

2. The Data Protection Officer shall maintain the confidentiality of the information and data received thereby in implementation of the duties and powers given thereto pursuant to the provisions of this Decree Law and the Executive Regulations thereof and in accordance with the legislation in force in the State.

Article 12 - Obligations of the Controller and Processor towards the Data Protection Officer

1. The Controller and Processor shall provide all means to ensure that the Data Protection Officer performs the responsibilities and duties assigned thereto, as stipulated in Article (11) hereof, in a proper manner, including, in particular, the following:
    - a. ensuring that he/she is appropriately and timely engaged in all matters relating to Personal Data Protection.
    - b. ensuring that he/she is provided with all the necessary resources and support to perform the duties assigned thereto.
    - c. not to terminate his/her service or impose any disciplinary penalty for a reason related to the performance of his/her duties in accordance with the provisions hereof.
    - d. ensuring that he/she is not assigned to duties that lead to a conflict of interest with the duties assigned thereto hereunder.
2. The Data Subject may communicate directly with the Data Protection Officer for any matters related to his/her Personal Data and the Processing thereof in order to exercise his/her rights in accordance with the provisions hereof.

Article 13 - Right to Obtain Information

1. The Data Subject, based on a request submitted thereby to the Controller, has the right to obtain the following information without charge:
    - a. the types of his/her Personal Data that is processed.
    - b. purposes of Processing.
    - c. decisions made based on Automated Processing, including Profiling.
    - d. targeted sectors or establishments with which his/her Personal Data is to be shared, whether inside or outside the State.
    - e. controls and standards for the periods of storing and keeping his/her Personal Data.
    - f. procedures for correcting, erasing or limiting the Processing and objection to his/her personal data.
    - g. protection measures for Cross-Border Processing made in accordance with Articles (22) and (23) hereof.
    - h. procedures to be taken in the event of a breach or infringement of his/her Personal Data, especially if the breach or infringement poses a direct and serious threat to the privacy and confidentiality of his/her Personal Data.
    - i. the process of filing complaints with the Office.
2. In all cases, the Controller shall, before starting the Processing, provide the Data Subject with the information stated in Paragraphs (B), (D) and (G) of Item (1) of this Article.
3. The Controller may refuse the Data Subject's request to obtain the information stated in Item (1) of this Article, if it is found out that:
    - a. the request is not related to the information referred to in Item (1) of this Article or is excessively repetitive.
    - b. the request conflicts with the judicial procedures or investigations made by the competent authorities.
    - c. the request may adversely affect the efforts of the Controller to protect information security.
    - d. the request affects the privacy and confidentiality of the Personal Data of others.

Article 14 - Right to Request Personal Data Transfer

1. The Data Subject has the right to obtain his/her Personal Data provided to the Controller for Processing in a structured and machine-readable manner, so long as the Processing is based on the Consent of the Data Subject or is necessary for the fulfillment of a contractual obligation and is made by automated means.
2. The Data Subject has the right to request the transfer of his/her Personal Data to another Controller whenever this is technically feasible.

Article 15 - Right to Correction or Erasure of Personal Data

1. The Data Subject has the right to request the correction or completion of his/her inaccurate Personal Data held with the Controller without undue delay.

2. Without prejudice to the legislation in force in the State and what is required by the public interest, the Data Subject has the right to request the erasure of his/her Personal Data held with the Controller in any of the following cases:
    - a. if his/her Personal Data is no longer required for the purposes for which it is collected or processed.
    - b. if the Data Subject withdraws his/her Consent on which the Processing is based.
    - c. if the Data Subject objects to the Processing or if there are no legitimate reasons for the Controller to continue the Processing.
    - d. if his/her Personal Data is processed in violation of the provisions hereof and the legislation in force, and the erasure process is necessary to comply with the applicable legislation and approved standards in this regard.
3. With the exception of what is stated in Item (2) of this Article, the Data Subject has no right to request erasure of his /her Personal Data held with the Controller in the following cases:
    - a. if the request is for the erasure of his/her Personal Data related to public health and held with private establishments.
    - b. if the request affects the investigation procedures, claims for rights and legal proceedings or defense by the Controller.
    - c. if the request conflicts with other legislation to which the Controller is subject.
    - d. any other cases set by the Executive Regulations of this Decree Law.

Article 16 - Right to Restrict Processing

1. The Data Subject has the right to oblige the Controller to restrict and stop Processing in any of the following cases:
    - a. if the Data Subject objects to the accuracy of his/her Personal Data, in which case the Processing shall be restricted to a specific period allowing the Controller to verify accuracy of the data.
    - b. if the Data Subject objects to the Processing of his/her Personal Data in violation of the agreed purposes.
    - c. if the Processing is made in violation of the provisions hereof and the legislation in force.
2. The Data Subject has the right to request the Controller to continue to keep his/her Personal Data after fulfillment of the purposes of Processing, if such data is necessary to complete procedures related to claiming or defending rights and legal proceedings.
3. Notwithstanding the provisions of Item (1) of this Article, the Controller may proceed with the Processing of the Personal Data of the Data Subject without his/her Consent in any of the following cases:
    - a. if the Processing is limited to storing Personal Data.
    - b. if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial procedures.
    - c. if the Processing is necessary to protect the rights of third parties in accordance with the legislation in force.
    - d. if the Processing is necessary to protect the public interest.
4. In all cases, the Controller shall notify the Data Subject in the event of lifting the restriction stipulated in this Article.

Article 17 - Right to Stop Processing

The Data Subject has the right to object to and stop the Processing of his/her Personal Data in any of the following cases:

1. if the Processing is for direct marketing purposes, including Profiling related to direct marketing.
2. if the Processing is for the purposes of conducting statistical surveys, unless the Processing is necessary to achieve the public interest.
3. if the Processing is in violation of the provisions of Article (5) hereof.

Article 18 - Right to Processing and Automated Processing

1. The Data Subject has the right to object to decisions issued with respect to Automated Processing that have legal consequences or seriously affect the Data Subject, including Profiling.
2. Notwithstanding the provisions of Item (1) of this Article, the Data Subject may not object to the decisions issued with respect to Automated Processing in the following cases:
    - a. if the Automated Processing is included in the terms of the contract entered into between the Data Subject and Controller.
    - b. if the Automated Processing is necessary according to other legislation in force in the State.
    - c. if the Data Subject has given his/her prior Consent on the Automated Processing in accordance with the conditions set out in Article (6) hereof.

3. The Controller shall apply appropriate procedures and measures to protect the privacy and confidentiality of the Personal Data of the Data Subject in the cases referred to in Item (2) of this Article, without prejudice to his/her rights.
4. The Controller shall engage human resources in reviewing Automated Processing decisions, at the request of the Data Subject.

Article 19 - Communication with the Controller

The Controller shall provide appropriate and clear ways and mechanisms to enable the Data Subject to communicate therewith and request the exercise of any of his/her rights stipulated herein.

Article 20 - Personal Data Security

1. The Controller and Processor shall establish and take appropriate technical and organizational measures and procedures to ensure achievement of the information security level that is commensurate with the risks associated with Processing, in accordance with the best international standards and practices, which may include the following:
    - a. encryption of Personal Data and application of Pseudonymization.
    - b. application of procedures and measures that ensure the confidentiality, safety, validity and flexibility of Processing systems and services.
    - c. application of procedures and measures that ensure the timely retrieval and access of Personal Data in the event of any physical or technical failure.
    - d. application of procedures that ensure a smooth testing, evaluation and assessment of the effectiveness of technical and organizational measures so as to ensure the security of Processing.
2. When evaluating the level of information security provided for in Item (1) of this Article, the following shall be taken into account:
    - a. risks associated with Processing, including Personal Data damage, loss, accidental or illegal modification, disclosure or unauthorized access, whether transmitted, stored or processed.
    - b. the costs, nature, scope and purposes of Processing, as well as the different potential risks to the privacy and confidentiality of the Personal Data of the Data Subject.

Article 21 - Assessment of Personal Data Protection Impact

1. Subject to the nature, scope and purposes of Processing, the Controller shall, before making the Processing, assess the impact of the proposed Processing on Personal Data Protection, when using any of the modern technologies that would pose a high risk to the privacy and confidentiality of the Personal Data of the Data Subject.
2. The impact assessment provided for in Item (1) of this Article shall be required in the following cases:
    - a. if the Processing involves a systematic and comprehensive assessment of the personal aspects of the Data Subject based on Automated Processing, including Profiling, which would have legal consequences or would seriously affect the Data Subject.
    - b. if the Processing will be made on a large amount of Sensitive Personal Data.
3. The assessment provided for in Item (1) of this Article must include, at a minimum, the following:
    - a. a clear and systematic explanation of the impact of the proposed Processing on Personal Data Protection and the purpose of such Processing.
    - b. an assessment of the necessity and suitability of Processing for the purpose thereof.
    - c. an assessment of the potential risks to the privacy and confidentiality of the Personal Data of the Data Subject.
    - d. the proposed procedures and measures to minimize the potential risks to Personal Data Protection.
4. The Controller may make a single assessment for a set of Processing operations of similar natures and risks.
5. The Controller shall coordinate with the Data Protection Officer when assessing the impact of Personal Data Protection.
6. The Office shall prepare a list of the types of Processing operations for which the assessment of the Personal Data Protection impact is not required and make it available to the public through its website.
7. The Controller shall review the assessment outcomes periodically to ensure that the Processing is carried out in accordance with the assessment, in case the levels of risks associated with the Processing operations are different.

Article 22 - Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is an Adequate Level of Protection

Personal Data may be transferred outside the State in the following cases approved by the Office:

1. if the country or territory to which the Personal Data is to be transferred has special legislation on Personal Data Protection therein, including the most important provisions, measures, controls, requirements and rules for protecting the privacy and confidentiality of the Personal Data of the Data Subject and his/her ability to exercise his/her rights, and provisions related to imposing appropriate measures on the Controller or Processor through a supervisory or judicial authority.
2. if the State accedes to bilateral or multilateral agreements related to Personal Data Protection with the countries to which the Personal Data is to be transferred.

Article 23 - Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is not an Adequate Level of Protection

1. With the exception of what is stated in Article (22) hereof, Personal Data may be transferred outside the State in the following cases:
    - a. In countries where there is no data protection law, Establishments operating in the State and in those countries may transfer data under a contract or agreement that obliges the Establishment in those countries to implement the provisions, measures, controls and requirements set out herein, including provisions related to imposing appropriate measures on the Controller or Processor through a competent supervisory or judicial authority in that country, which shall be specified in the contract.
    - b. The express Consent of the Data Subject to transfer his/her Personal Data outside the State in a manner that does not conflict with the security and public interest of the State.
    - c. If the transfer is necessary to fulfill obligations and establish, exercise or defend rights before judicial authorities.
    - d. If the transfer is necessary to enter into or execute a contract between the Controller and Data Subject, or between the Controller and a third party to achieve the Data Subject's interest.
    - e. If the transfer is necessary to perform a procedure relating to international judicial cooperation.
    - f. If the transfer is necessary to protect the public interest.
2. The Executive Regulations of this Decree Law shall set the controls and requirements for the cases referred to in Item (1) of this Article, which must be met for transferring Personal Data outside the State.

Article 24 - Filing a Complaint

1. The Data Subject may file a complaint with the Office if he/she has reasons to believe that any violation of the provisions hereof has occurred, or that the Controller or Processor processes his/her Personal Data in violation of the provisions hereof, in accordance with the procedures and rules established by the Office in this regard.
2. The Office shall receive the complaints filed by the Data Subject in accordance with Item (1) of this Article and verify them in coordination with the Controller and Processor.
3. The Office may impose the administrative penalties referred to in Article (26) hereof if it is proven that the Controller or Processor has violated the provisions of this Decree Law or the decisions issued in implementation thereof.

Article 25 - Grievances against the Office's Decisions

Any concerned party may submit a written grievance to the Office General Manager against any decision, administrative penalty or procedure taken against him/her by the Office, within thirty (30) days from the date of being notified of such decision, administrative penalty or procedure. The grievance shall be decided on within thirty (30) days from the date of its submission.

Any decision issued by the Office in implementation of the provisions hereof may not be appealed without filing a grievance against it. The Executive Regulations of this Decree Law shall set the procedures for filing grievances and deciding thereon.

Article 26 - Administrative Penalties and Violations

The Cabinet shall, based on the proposal of the Office General Manager, issue a decision specifying the acts that constitute a violation of the provisions of this Decree Law and the Executive Regulations thereof and the administrative penalties to be imposed.

Article 27 - Delegation

The Cabinet may, based on the proposal of the Office General Manager, delegate to any of the competent local government authorities, within their local jurisdiction, some of the powers entrusted to the Office hereunder.

Article 28 - Executive Regulations

The Cabinet shall, based on a proposal of the Office General Manager, issue the Executive Regulations of this Decree Law within six (6) months from the date of its promulgation.

Article 29 - Regularization

Controllers and Processors shall regularize their status in accordance with the provisions of this Decree Law within a period not exceeding six (6) months from the date of issuance of its Executive Regulations. The Cabinet may extend such period for another similar period.

Article 30 - Repeals

Any provision contrary to or in conflict with the provisions of this Decree Law shall be repealed.

Article 31 - Publication and Enforcement of the Decree Law

This Decree Law shall be published in the Official Gazette and shall come into force as of 2 January 2022 AD.

Issued by us, at the Presidential Palace in Abu Dhabi:

On: 13 Safar 1443 AH

Corresponding to: 20 September 2021 AD

Khalifa bin Zayed Al Nahyan

President of the United Arab Emirates