FEDERAL DECREE LAW NO. 45 OF 2021

ON PERSONAL DATA PROTECTION LAW

(which was issued on 20 September 2021)

This is an unofficial English translation for reference purposes only and should not be relied upon and does not constitute legal advice. The original Arabic version is the authoritative text and should always be referred to and for the purposes of interpretation the Arabic version should prevail.

FEDERAL DECREE LAW NO. 45 OF 2021

ON PERSONAL DATA PROTECTION LAW

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

having perused the Constitution;

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

Federal Decree Law No. 3 of 2003 on the Regulation of Telecommunication Sector, as amended;

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

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

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

Federal Decree Law No. 14 of 2018 on the Central Bank and the Regulation of Financial Institutions and Activities, as amended;

Federal Decree Law No. 44 of 2021 on the Establishment of the UAE Data Office; and

upon the proposal of the Minister of Cabinet Affairs and the approval of the Cabinet,

have promulgated the following Decree Law:

ARTICLE (1)

DEFINITIONS

In applying the provisions of this Decree Law and unless the context otherwise requires, the following terms and expressions shall have the meanings ascribed thereto below:

State	:	The United Arab Emirates.
Office	:	The Data Office established under Federal Decree Law No. 44 of 2021 referred to above.
Data	:	A set of organised or unorganised information, facts, concepts, instructions, observations or measurements taking the form of figures, letters, words, codes, photos, videos, signals, sounds, charts or otherwise, that are interpreted, exchanged or processed by individuals or computers, including information wherever mentioned herein.

Personal Data	: Any information relating to an identified natural person or to a natural person who can be identified, directly or indirectly, in particular by Data linking and reference to an identifier such as a name, voice, photo, an identification number, an online identifier, location data or to one or more factors specific to the physical, physiological, economic, cultural or social identity of that natural person, which expression includes the "Sensitive Personal Data" and "Biometric Data".
Sensitive Personal Data	: Any information that reveals, either directly or indirectly, a natural person's family, racial origin, political, philosophical, or religious beliefs, criminal records, Biometric Data, or any information concerning the health of such person, including the physical, psychological, mental, genetic or sexual status of such person, including the provision of health care services, which reveal information about his or her health status.
Biometric Data	: Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a Data Subject, which allow or confirm the unique identification of that Data Subject, such as facial images or dactyloscopic data.
Data Subject	: The natural person who is the subject of Personal Data.
Entity	: Any incorporated or unincorporated entity inside or outside the State, including companies which are partially or wholly owned by the federal or local government or in which the federal or local government is a shareholder.
Controller	: The Entity or the natural person who obtains Personal Data and who, by virtue of their activity, determines, whether alone or jointly with other persons or Entities, the method, means, criteria and purposes of the Processing of such Personal Data.
Processor	: The Entity or the natural person who processes Personal Data on behalf of the Controller, where such Processing is being carried out under the supervision of, and as directed by, the Controller.
Data Protection Officer	: A natural or legal person appointed by the Controller or the Processor to monitor the compliance of the employer of such officer with the controls, requirements, procedures and rules of the Processing and protection of Personal Data provided for in this Decree Law, and to ensure the integrity of the systems and procedures of

such employer to ensure compliance with the provisions hereof.

Processing : Any operation or set of operations which is performed on Personal Data, whether by automated means, including the method of Processing, or otherwise, and such operation(s) include(s) the collection, storage, recording, organisation, adaptation, modification, circulation, alternation, retrieval, exchanging, sharing, use, characterisation, disclosure by transmission, dissemination, distribution, or otherwise making available, alignment or combination, restriction, withholding, erasure, destruction or creating models of Personal Data.

Automated Processing : The Processing that is performed by a software or an electronic system that operates automatically, whether totally independently without any human involvement or partially with a limited human supervision and involvement.

Personal Data Security : A set of technical and organisational measures, procedures and operations as specified hereunder which ensures the protection of the privacy, confidentiality, integrity, unity, integration and availability of Personal Data.

Pseudonymisation : The Processing of Personal Data in such a manner that the Personal Data processed as such can no longer be attributed to the Data Subject without the use of additional information, provided that such additional information is kept separately and safely and is subject to the technical and organisational measures provided for herein to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Anonymisation : The Processing that is performed on Personal Data in such as a matter that a Data Subject is no longer identifiable and such Data can no longer be attributed to or otherwise identify such Data Subject.

Data Breach : A breach of security and Personal Data by unlawful or unauthorised access thereto, including the reproduction, transmission, dissemination, exchange, transfer, circulation, or the Processing of Personal Data in a matter that leads to its disclosure to a third party, or the destruction or alteration of Personal Data while being transmitted, stored or processed.

Profiling	:	Any form of Automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a Data Subject, in particular to analyse or predict aspects concerning that Data Subject's performance [at work], economic situation, health, personal preferences, interests, behaviour, location, movements or reliability.
Cross-Border Processing	:	The publishing, use, display, transmission, receipt, retrieval, utilisation, sharing or Processing of Personal Data outside the territory of the State.
Consent	:	The consent whereby a third party is permitted by the Data Subject to process the Personal Data of such Data Subject, provided that such Consent must give a specific, clear and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of his/her Personal Data.

ARTICLE (2)

SCOPE OF APPLICATION

1. The provisions of this Decree Law shall apply to the Processing of Personal Data, wholly or partially by automated means or otherwise by:
   (a) every Data Subject who resides or has a place of business in the State;
   (b) every Controller or Processor in the State who carries out the activity of Processing the Personal Data of Data Subjects inside and outside the State;
   (c) every Controller or Processor not established in the State who carries out the activity of Processing the Personal Data of Data Subjects in the State;
2. The provisions of this Decree Law shall not apply to:
   (a) The government data
   (b) The government authorities which control or process Personal Data.
   (c) The Personal Data maintained by security and judicial authorities.
   (d) The Processing by a Data Subject of his/her own Data for personal purposes.
   (e) Health Personal Data the protection and Processing of which is governed by another legislation.

(f) Bank and credit Personal Data and Information the protection and Processing of which is governed by another legislation.

(g) Companies and establishments established in the free zones in the State, which are subject to their respective Personal Data protection regulations.

ARTICLE (3)

THE AUTHORITY OF THE OFFICE TO GRANT EXEMPTIONS

Without prejudice to any other functions entrusted to the Office pursuant to any other legislation, the Office may exempt certain Entities which do not process a large scale of Personal Data from part or all of the requirements and conditions of the provisions of Personal Data protection set out in this Decree Law, subject to the criteria and controls set out in the executive regulations of this Decree Law.

ARTICLE (4)

UNCONSENTED PROCESSING OF PERSONAL DATA

No Personal Data may be processed without the Consent of the Data Subject to which such Data relates. Such prohibition shall not apply in the following events, in which case the Processing will be lawful:

1. Processing is necessary for the protection of the public interest;
2. Processing relates to Personal Data which are manifestly made public by the Data Subject;
3. Processing is necessary for the establishment, exercise or defence of rights and legal claims or relates to judicial or security measures;
4. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care or treatment, or the management of health or social care systems and services in accordance with the legislation in force in the State;
5. Processing is necessary for protecting the public health, such as protecting against communicable diseases and pandemics or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of the legislation in force in the State;
6. Processing is necessary for archiving purposes, scientific or historical research purposes or statistical purposes in accordance with the legislation in force in the State;
7. Processing is necessary to protect the interests of the Data Subject;
8. Processing is necessary for the purposes of carrying out the obligations and exercising the rights prescribed by law for the Controller or of the Data Subject in the field of

employment, social security and social protection law in so far as it is authorised by such laws;

9. Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject for entering into, amending or terminating a contract;
10. Processing is necessary for the performance by the Controller of specific obligations prescribed by other laws in the State;
11. any other event as set forth in the executive regulations of this Decree Law.

ARTICLE (5)

PROCESSING OF PERSONAL DATA RULES

Personal Data shall be processed in accordance with the following rules:

1. Processing shall be performed lawfully, fairly and in a transparent manner.
2. Personal Data shall be collected for specified and explicit purposes and not further processed in a manner that is incompatible with those purposes; further Processing for any other purposes is permissible if they are similar or relevant to the purposes for which such data are originally collected.
3. Personal Data shall be adequate and limited to what is necessary in relation to the purposes for which they are processed;
4. Personal Data shall be accurate and, where necessary, kept up to date;
5. Every reasonable step must be taken to ensure that Personal Data that are inaccurate are erased or rectified;
6. Personal Data shall be kept in a manner that ensures appropriate security of the Personal Data, including protection against any infringement, breach or unauthorised or unlawful processing, using appropriate technical or organisational measures in accordance with the applicable laws and legislation this regard;
7. Personal Data shall not be kept after the completion of the purpose for which such Data are processed, provided that such Data may be further kept if its Data Subject can no longer be identifiable through the use of “Anonymization” technique;
8. Any other controls as set forth in the executive regulations of this Decree Law.

ARTICLE (6)

CONDITIONS OF CONSENT TO THE PROCESSING OF DATA

1. For the Consent of a Data Subject to the Processing of his/her Data to be valid, the following conditions must be met:

(a) Where Processing is based on the Consent of the Data Subject, the Controller shall be able to demonstrate that the Data Subject has consented to the Processing of his or her Personal Data.

(b) The [request for] Consent, whether in written or electronic form, shall be prepared in a clear and simplified manner and in an intelligible and easily accessible form.

(c) The Consent shall include an indication to the right of the Data Subject to withdraw such Consent. It shall be easy to withdraw such Consent.

2. The Data Subject may, at any time, withdraw his/her Consent for the Processing of the Personal Data of the Data Subject. The withdrawal of Consent shall not affect the lawfulness of Processing based on Consent before its withdrawal.

ARTICLE (7)

GENERAL OBLIGATIONS OF THE CONTROLLER

The Controller shall:

1. implement appropriate technical and organisational measures to apply the standard criteria necessary to protect and secure Personal Data, to maintain its confidentiality and privacy and to ensure that such Data is not breached, destroyed, altered or tampered with, taking into account the nature, scope and purposes of Processing as well as the potential risks to the confidentiality and privacy of the Personal Data of the Data Subject;

2. both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate measures, such as Pseudonymisation, in order to meet the requirements of this Decree Law, including those set out in Article (5) hereof;

3. implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. That obligation applies to the amount and type of Personal Data collected, the type of their Processing, the period of their storage and their accessibility;

4. keep a register of Personal Data, which shall include the details of the Controller and Data Protection Officer, a statement setting out the categories of Personal Data kept by the Controller, the details of the persons who are authorized to access the Personal Data, the duration, restrictions and scope of Processing, the mechanism for the erasure, modification or Processing of Personal Data by the Controller, the purpose of Processing, and any details on the Cross-Border Processing and movement of Personal Data, and a statement setting out the technical and organisational measures relating to information security and Processing operations. The Controller shall make such register available to the Office upon request;

5. appoint a Processor providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the

Processing rules and requirements set forth in this Decree Law, its executive regulations and the decisions issued in implementation thereof;

6. provide the Office, upon a decision by the competent judicial authority, with any information requested by the Office to exercise the powers granted thereto under this Decree Law and its executive regulations;

7. perform any other obligations as set out in the executive regulations of this Decree Law.

ARTICLE (8)

GENERAL OBLIGATIONS OF THE PROCESSOR

The Processor shall:

1. perform and implement the Processing based on the instructions of the Controller and in accordance with the contracts and agreements entered into between them, which shall specifically set out the scope, subject-matter, purpose and nature of the Processing, the type of Personal Data, and categories of Data Subjects;

2. both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organisational measures to ensure data protection by design, taking into account the cost of implementation and the nature, scope and purposes of Processing;

3. perform the Processing according to its purpose and duration and shall, if the Processing runs beyond the duration specified thereof, inform the Controller of the same to authorise the extension of such duration or to issue the appropriate instructions;

4. delete or return the Personal Data to the Controller after the end of the Processing duration;

5. not do any act that would lead to the disclosure of Personal Data or the results of Processing except as otherwise permitted by law;

6. protect and secure the Processing and secure the electronic media and equipment used in the Processing operations and the Personal Data stored therein;

7. keep a register of the Personal Data processed on behalf of the Controller, provided that such register shall include the details of the Controller, the Processor and the Data Protection Officer, a statement setting out the categories of Personal Data kept by the Processor, the details of the persons who are authorized to access the Personal Data, the duration, restrictions and scope of Processing, the mechanism for the erasure, modification or Processing of Personal Data by the Processor, the purpose of Processing, and any details on the Cross-Border Processing and movement of Personal Data, and a statement setting out the technical and organisational measures relating to information security and Processing operations. The Processor shall make such register available to the Office upon request;

8. provide, upon the request of the Controller or the Office, all means necessary to demonstrate compliance with the provisions of this Decree Law;

9. perform and implement the Processing in accordance with the rules and requirements which are set out in this Decree Law or its executive regulations or under which instructions by the Office are issued;

10. Where more than one Processor is engaged in the Processing, such Processing shall be performed in accordance with a contract or agreement in writing, which clearly sets out their respective obligations, responsibilities and roles in the Processing; otherwise they shall be jointly liable for the obligations and responsibilities set out in this Decree Law and its executive regulations.

11. The executive regulations of this Decree Law shall set out the procedures, controls, conditions and the technical and standard criteria relating to such obligations

ARTICLE (9)

NOTIFICATION OF DATA BREACHES

1. In addition to the obligations of the Controller set out in this Decree Law, in the case of a Data Breach that would prejudice the privacy, confidentiality and security of the Personal Data of a Data Subject, the Controller shall, immediately upon becoming aware of such Breach, notify the Office of such Data Breach and the findings of the investigation. Such notification shall be made within the time limit and in accordance with the procedures and conditions set forth in the executive regulations of this Decree Law. Such notification shall be accompanied by the following information and documents:

   (a) A description of the nature, category, reasons, approximate number and records of the Data Breach[1];

   (b) The details of the Data Protection Officer appointed by the Controller;

   (c) A description of the likely consequences of the Data Breach;

   (d) A description of the measures taken or proposed to be taken by the Controller to address the Data Breach and to mitigate its possible adverse effects;

   (e) Documenting the Data Breach and the remedial action taken;

   (f) Any other requirements requested by the Office.

2. At all events, when the Personal Data Breach is likely to prejudice the privacy, confidentiality and security of the Personal Data of a Data Subject, the Controller shall communicate the Data Breach and the measures taken by the Controller to the Data Subject concerned. Such notification shall be made within the time limit and in accordance with the procedures and conditions set forth in the executive regulations of this Decree Law.

3. The Processor shall notify the Controller of any Personal Data Breach upon becoming aware of such breach. The Controller shall in turn notify the Office in accordance with paragraph (1) of this Article.

4. Upon the receipt of such notification from the Controller, the Office shall investigate the reasons of such breach to ensure the integrity of the security measures taken, and shall, in case of proven violation of the provisions of this Decree Law and the decisions issued in implementation thereof, impose the administrative sanctions referred to in Article (26) of this Decree Law.

ARTICLE (10)

DESIGNATION OF THE DATA PROTECTION OFFICER

1. The Controller and the Processor shall designate a Data Protection Officer based on professional qualities and expert knowledge of Personal Data Protection in any case where:

   (a) a type of Processing that is using new technologies or is based on the scale of Data is likely to result in a high risk to the confidentiality and privacy of the Personal Data of a Data Subject;

   (b) Processing includes a systematic and extensive evaluation of Sensitive Personal Data, including Profiling and Automated Processing;

   (c) Processing is performed on a large scale of Sensitive Personal Data;

2. The Data Protection Officer may be a staff member of, or may be authorized by, the Controller or Processor, whether based inside or outside the State.

3. The Controller or the Processor shall specify and communicate the contact details of the Data Protection Officer to the Office.

4. The executive regulations of this Decree Law shall set out the types of technologies and the criteria for determining the scale of Data required pursuant to this Article.

ARTICLE (11)

TASKS OF THE DATA PROTECTION OFFICER

1. The Data Protection Officer shall ensure compliance by the Controller or the Processor with the provisions of this Decree Law, its executive regulations and the instructions issued by the Office. The Data Protection Office shall, in particular, have the following tasks and powers:

   (a) to verify the quality and integrity of measures adopted by the Controller and the Processor;

   (b) to receive applications and complaints relating to Personal Data in accordance with the provisions of this Decree Law and its executive regulations;

   (c) to provide technical advice as regards the assessment and periodic review of the Personal Data protection systems of the Controller and the Processor, and Data Breaches prevention systems, to document the results of such assessment and to

provide the appropriate recommendations on the same, including the risk assessment procedures;

(d) to act as the contact point between the Controller or the Processor, as the case may be, and the Office on their compliance with the provisions of Processing of Personal Data stipulated in this Decree Law;

(e) to perform or exercise any other tasks or powers as set out in the executive regulations of this Decree Law.

2. The Data Protection Officer shall keep confidential any information and data received by such Officer for the performance of his/her tasks and powers in accordance with the provisions of this Decree Law, its executive regulations and the legislation in force in the State.

ARTICLE (12)

DUTIES OF THE CONTROLLER AND PROCESSOR TOWARDS THE DATA PROTECTION OFFICER

1. The Controller and Processor shall provide the Data Protection Officer with all means necessary to properly perform the tasks assigned thereto as set out in Article 11 of this Decree Law. The Controller and Processor shall, in particular:

(a) ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data;

(b) ensure that the Data Protection Officer is provided with the resources and support necessary to carry out his tasks;

(c) not dismiss or penalize the Data Protection Officer for performing his tasks in accordance with the provisions of this Decree Law;

(d) ensure that the Data Protection Officer is not entrusted with tasks that result in a conflict of interests with his tasks hereunder.

2. Data subjects may directly contact the Data Protection Officer with regard to all issues related to the Processing of their Personal Data so they can exercise their rights under this Decree Law.

ARTICLE (13)

RIGHT TO OBTAIN INFORMATION

1. The Data Subject shall, upon a request to the Controller, have the right to obtain, free of charge, the following information:

(a) the types of Personal Data of the Data Subject being processed;

(b) the purposes of the Processing;

(c) the decisions taken on the basis of Automated Processing, including Profiling;

(d) the targeted sectors or Entities inside or outside the State with whom his Personal Data will be shared;

(e) the rules and criteria of the periods for which the Personal Data will be stored and kept;

(f) the procedures for the rectification, erasure or restriction of Processing and objecting to his/her Personal Data[2];

(g) the appropriate safeguards for Cross-Border Processing which is carried out in accordance with Article 22 and 23 of this Decree Law;

(h) the measures to be taken upon the occurrence of a Data Breach, particularly if any such breach is likely to result in a direct and high risk to the privacy and confidentiality of Personal Data of the Data Subject;

(i) how to lodge a complaint with the Office;

2. At all events, the Controller shall provide the Data Subject, prior to the start of Processing activities, with the information referred to in points (b), (d) and (g) of paragraph (1) of this Article.

3. The Controller may reject the request of the Data Subject to obtain the information referred to in paragraph (1) of this Article if it appears to the Controller that:

(a) the request is not relevant to the information referred to in paragraph (1) of this Article or is excessively frequent;

(b) the request conflicts with judicial proceedings or investigations carried out by the competent authorities;

(c) the request may adversely affect the efforts by the Controller to protect data security.

(d) the request may prejudice the privacy and confidentiality of the Personal Data of a third party.

ARTICLE (14)

RIGHT TO PERSONAL DATA PORTABILITY

1. The Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to a Controller for Processing, in a structured and machine-readable format where the Processing is based on the Consent of the Data

Subject, or is necessary to fulfil a contractual obligation and implemented by automated means.

2. The Data Subject shall have the right to have his/her Personal Data transmitted to another Controller, where technically feasible.

ARTICLE (15)

RIGHT TO RECTIFICATION AND ERASURE OF PERSONAL DATA

1. The Data Subject shall have the right to obtain from the Controller, without undue delay, the rectification of inaccurate Personal Data concerning him or her, and to have incomplete Personal Data completed.
2. Without prejudice to the legislation in force in the State and as dictated by the public interest, the Data Subject shall have the right to obtain from the Controller the erasure of Personal Data concerning him or her in any of the following events:
   (a) his/her Personal Data are no longer necessary in relation to the purposes for which they were collected or processed;
   (b) the Data Subject withdraws Consent on which the processing is based;
   (c) the Data Subject objects to the Processing and there are no legitimate grounds for the Controller to continue the Processing;
   (d) the Personal Data have been processed in violation of the provisions of this Decree Law and the legislation in force and have to be erased for compliance with the applicable legislation and the criteria adopted in this regard;
3. Notwithstanding the provisions of paragraph (2) of this Article, the Data Subject may not obtain from the Controller the erasure of Personal Data concerning him or her in any of the following events:
   (a) where the request is for the erasure of Personal Data maintained by private Entities in relation to public health;
   (b) where the request affects any investigations, claim of rights and legal claims or the defence of the same by the Controller;
   (c) where the request conflicts with other legislation to which the Controller is subject;
   (d) any other events set forth in the executive regulations of this Decree Law.

ARTICLE (16)

RIGHT TO RESTRICT PROCESSING

1. The Data Subject shall have the right to obtain from the Controller restriction and suspension of Processing where one of the following applies:

(a) the accuracy of the Personal Data is contested by the Data Subject, in which case the Processing will be suspended for a period enabling the Controller to verify the accuracy of the Personal Data;

(b) the Data Subject has objected to the Processing of his/her Personal Data for any purpose other than the purposes agreed to;

(c) the Processing is performed in violation of the provisions of this Decree Law and the legislation in force.

2. Where the Personal Data are necessary to finalise any actions relating to the exercise or defence of any rights or legal claims, the Data Subject shall have the right to request the continued retention of his Personal Data by the Controller after the completion of the objectives of Processing.

3. Notwithstanding the provisions of paragraph (1) of this Article, the Controller may proceed with the Processing of Personal Data without the Consent of the Data Subject where:

(a) the Processing is limited to the storage of the Personal Data;

(b) the Processing is necessary for the establishment, exercise or defence of rights and legal claims or relates to judicial proceedings;

(c) the Processing is necessary to protect the rights of a third party pursuant to the legislation in force;

(d) the Processing is necessary for the protection of the public interest.

4. At all events, where the restriction referred to in this Article is lifted by the Controller, the Controller shall inform the Data Subject of the same.

ARTICLE (17)

RIGHT TO SUSPEND PROCESSING

The Data Subject shall have the right to object to and suspend the Processing of Personal Data concerning him or her where:

1. the Processing is performed for direct marketing purposes, including Profiling to the extent that it is related to such direct marketing;

2. the Processing is performed for statistical surveys purposes, unless the Processing is necessary for reasons of public interest;

3. the Processing is performed in violation of the provisions of Article 5 of this Decree Law.

ARTICLE (18)

RIGHT TO PROCESSING AND AUTOMATED PROCESSING

1. The Data Subject shall have the right to object to decisions based on Automated Processing, including Profiling, particularly any such decision which produces legal effects or similarly significantly affects him or her.

2. Notwithstanding the provisions of paragraph (1) of this Article, the Data Subject shall not have the right to object to decisions based on Automated Processing where:

   (a) the Automated Processing is stipulated in a contract between the Data Subject and the Controller;

   (b) the Automated Processing is necessary under any other legislation in force in the State;

   (c) the Automated Processing is based on a prior Consent by the Data Subject in accordance with requirements set out in Article (6) of this Decree Law;

3. In the cases referred to in paragraph (2) of this Article, the Controller shall implement suitable measures to safeguard the privacy and confidentiality of the Data Subject's Personal Data and not to prejudice his/her rights.

4. The Data Subject shall have the right to obtain human intervention on the part of the Controller to review any decisions based on Automated Processing.

ARTICLE (19)

MEANS OF COMMUNICATION WITH THE CONTROLLER

The Controller shall provide appropriate and clear means and mechanisms to enable Data Subjects to communicate with the Controller and to request the exercise of any of their rights under this Decree Law.

ARTICLE (20)

SECURITY OF PERSONAL DATA

1. The Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by Processing in accordance with the international best standards and practices, including:

   (a) the encryption and Pseudonymisation of Personal Data;

   (b) the implementation of measures to ensure the ongoing confidentiality, integrity, accuracy and resilience of Processing systems and services;

(c) the implementation of measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) the implementation of a process to ensure a seamless testing, assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of the Processing.

2. In assessing the level of security referred to in paragraph (1) of this Article, the following shall be taken into account:

(a) the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or processed;

(b) the costs of implementation and the nature, scope and purposes of Processing as well as the risk of varying likelihood to the privacy and confidentiality of the Personal Data of the Data Subject.

ARTICLE (21)

PERSONAL DATA PROTECTION IMPACT ASSESSMENT

1. Where a type of processing using new technologies that is likely to result in a high risk to the privacy and confidentiality of the Personal Data of a Data Subject, and taking into account the nature, scope and purposes of the Processing, the Controller shall, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data.

2. A data protection impact assessment referred to in paragraph 1 of this Article shall be required in the event that:

(a) the Processing involves a systematic and extensive evaluation of personal aspects relating to the Data Subject which is based on Automated Processing, including Profiling, and which produces legal effects concerning the Data Subject or similarly significantly affects the Data Subject;

(b) the Processing is carried out on a large scale of Sensitive Personal Data.

3. The assessment referred to in paragraph 1 of this Article shall contain at least:

(a) a clear and systematic description of the envisaged Processing operations as to the protection of Personal Data and the purposes of the Processing;

(b) an assessment of the necessity and proportionality of the Processing operations in relation to the purposes;

(c) an assessment of the potential risks to the privacy and confidentiality of the Personal Data of the Data Subject;

(d) the measures envisaged to address the risks to the protection of Personal Data.

4. The Controller may carry out a single assessment that addresses a set of similar Processing operations that are similar in nature and risks.

5. The Controller shall liaise with the Data Protection Officer when carrying out a Personal Data protection impact assessment.

6. The Office may establish and make public on its website a list of the kind of Processing operations for which no Personal Data protection impact assessment is required.

7. The Controller shall carry out a periodic review of the assessment results to assess if Processing is performed in accordance with such assessment when there is a change of the risk represented by Processing operations.

ARTICLE (22)

CROSS-BORDER TRANSFER OF PERSONAL DATA FOR PROCESSING PURPOSES WHERE AN ADEQUATE LEVEL OF PROTECTION IS AFFORDED

The transfer of Personal Data outside the State shall take place in the following events approved by the Office when:

1. the country or territory to which the Personal Data will be transferred has legislations in place for the protection of Personal Data, which shall include key provisions, measures, controls, requirements and rules for the protection of the privacy and confidentiality of the Personal Data of a Data Subject, and the ability of Data Subjects to exercise their rights, and provisions relating to the application of appropriate measures against the Controller or the Processor by a regulatory or judicial authority.

2. The accession by the State to bilateral or multilateral treaties relating to the protection of Personal Data with the countries to which the Personal Data will be transferred.

ARTICLE (23)

CROSS-BORDER TRANSFER OF PERSONAL DATA FOR PROCESSING PURPOSES WHERE AN ADEQUATE LEVEL OF PROTECTION IS NOT AFFORDED

1. Notwithstanding the provisions of Article (22) of this Decree Law, the Personal Data may be transferred outside the State where:

   (a) the transfer is made to countries having no data protection law in place, the companies operating in the State and such countries may transfer data under a contract or agreement whereby the company in such country will be required to apply the provisions, measures, controls and requirements set forth in this Decree Law, including the provisions relating to taking the necessary measures against the Controller or the Processor by the competent regulatory or judicial authority in such country as set out in such contract;

(b) the Data Subject has explicitly consented to the transfer of their Personal Data outside the territory of the State, to the extent that the same is not in conflict with the public and security interest of the State;

(c) the transfer is necessary for the performance of an obligation or the establishment, exercise or defence of rights before judicial authorities;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the Data Subject between the Controller and the Data Subject or between the Controller and a third party;

(e) the transfer is necessary for implementation of a procedure relating to an international judicial cooperation;

(f) the transfer is necessary for the protection of the public interest;

2. The executive regulations of this Decree Law shall set out the controls and conditions referred to in paragraph (1) of this Article, which must be fulfilled when Personal Data are being transferred outside the State.

ARTICLE (24)

FILING COMPLAINTS

1. Subject to the procedures and rules specified by the Office in this regard, the Data Subject may lodge a complaint with the Office if he has reason to believe that a violation of the provisions of this Decree Law is committed, or that the Processing by the Controller or the Processor infringes this Decree Law.

2. The Office shall receive the complaints lodged by Data Subjects in accordance with paragraph (1) of this Article, verify such complaints in liaison with the Controller and Processor.

3. In case of a proven violation of the provisions hereof and the decisions issued in implementation hereof, the Office shall apply the administrative sanctions referred to in Article (26) of this Decree Law.

ARTICLE (25)

FILING A COMPLAINT AGAINST THE DECISIONS OF THE OFFICE

Any interested person may, within thirty (30) days of being notified of any decision, sanction or action taken by the Office against such person, lodge a complaint in writing to the director general of the Office against any such decision, sanction or action. A decision on such complaint shall be issued within thirty (30) days of lodging such complaint.

No decision issued by the Office pursuant to the provisions of this Decree Law may be appealed unless a complaint is first lodged against such decision. The executive regulations of this Decree Law shall set out the procedures for filing and issuing a decision on any such complaints.

ARTICLE (26)

ADMINISTRATIVE SANCTIONS AND VIOLATIONS

The Cabinet shall, upon the proposal of the director general of the Office, issue a decision setting out the acts that constitute a violation of the provisions of this Decree Law and its executive regulations, and the administrative sanctions to be applied.

ARTICLE (27)

DELEGATION

The Cabinet may, upon the proposal of the director general of the Office, delegate some of the powers vested in the Office hereunder to any competent local government authority within its own competence.

ARTICLE (28)

EXECUTIVE REGULATIONS

The Cabinet shall, upon the proposal of the director general of the Office, issue the executive regulations for implementing the provisions of this Decree Law within six (6) months from the date of issuance of this Decree Law.

ARTICLE (29)

REGULARISATION OF STATUS

The Controller and Processor shall, within no later than six (6) months from the date of the issuance of the executive regulations of this Decree Law, regularise their statuses to ensure compliance with the provisions of this Decree Law. The Cabinet may extend such period for a similar period.

ARTICLE (32)

REVOCATION

Any provision that is contrary to or inconsistent with this Decree Law shall hereby be repealed.

ARTICLE (33)

PUBLICATION AND ENFORCEMENT OF THE LAW

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

Khalifa bin Zayed Al Nahyan

President of the United Arab Emirates

Issued by us at the Presidential Palace in Abu Dhabi

On: 13 Safar 1443H., corresponding to 20 September 2021