# Federal Decree by Law No. (45) of 2021

# Concerning the Protection of Personal Data

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

Having reviewed the Constitution; and

- Federal Law No. (1) of 1972 concerning the Competences of Ministries and the Powers of Ministers, and any amendments thereto; and
- Federal Decree by Law No. (3) of 2003 on Regulating the Telecommunications Sector, as amended; and
- Federal Law No. (6) of 2010 on Credit Information, as amended; and
- Federal Law No. (14) of 2016 on Administrative Violations and Penalties in the Federal Government; and
- Federal Law No. (2) of 2019 on the Use of Information and Communication Technology in the Health Fields; and
- Federal Decree by Law No. (14) of 2018 on the Central Bank and Regulation of Financial Institutions and Activities, and any amendments thereof; and
- Federal Decree by Law No. (44) of 2021 on the Establishment of the UAE Data Office; and
- Pursuant to what was presented by the Minister of Cabinet Affairs, and the approval of the Council of Ministers,

**have promulgated the following Decree by Law:**

## Article (1)

## Definitions

In application of the provisions of this Decree by Law, the following words and phrases shall have the meanings assigned to each of them, unless the context otherwise requires:

| | | |
|---|---|---|
| **State** | : | The United Arab Emirates |
| **Office** | : | The UAE Data Bureau established under the aforementioned Federal Decree by Law No. (44) of 2021 |
| **Data** | : | An organized or unorganized set of data, facts, concepts, instructions, observations or measurements in the form of numbers, letters, words, symbols, images, videos, signs, sounds, maps or any other form. It is interpreted, exchanged or processed by individuals or computers. It includes information wherever it appears herein. |
| **Personal Data** | : | Any data related to a specific natural person or related to a natural person that can be identified directly or indirectly by linking the data, through the use of identification elements such as his/her name, voice, image, identification number, his/her electronic identifier, his/her geographical location, or by one or more physical, physiological, economic, cultural or social characteristics. It includes Sensitive Personal Data and Biometric Data |
| **Sensitive Personal Data** | : | Any data which directly or indirectly reveals a natural person's family, ethnic origin, political or philosophical opinions, religious beliefs, criminal record, biometric data, or any data relating to such |

| | | |
|---|---|---|
| | | person's health and physical, psychological, mental, genetic or sexual condition, including information related to the provision of healthcare services to him/her which reveals his/her health status |
| **Biometric Data** | : | Personal Data resulting from processing using a specific technology related to the physical, physiological or behavioral characteristics of the Data Subject, which allows the identification or confirmation of the unique identification of the Data Subject, such as facial images or fingerprints |
| **Data Subject** | : | A Natural Person who is the subject of Personal Data |
| **Establishment** | : | Any individual company or establishment located inside or outside the State, including companies wholly owned by the federal or the local government, or in which they are shareholders |
| **Controller** | : | An establishment or natural person that has Personal Data, and by virtue of its activity, determines whether individually or jointly with other persons or establishments, the method and criteria for processing such Personal Data and the purpose of processing it |
| **Processor** | : | An establishment or Natural Person that processes Personal Data on behalf of the Controller. It processes it under their supervision and in accordance with their instructions |
| **Data Protection Officer** | : | Any Natural or Legal Person appointed by the Controller or Processor, that undertakes the tasks of ascertaining the extent to which the entity to which it belongs complies with the controls, requirements, procedures and rules for processing Personal Data |

| | | |
|---|---|---|
| | | Protection stipulated herein. It also ensures the integrity of systems and procedures in order to achieve compliance with provisions of the Decree by Law |
| **Processing** | : | Any operation or set of operations performed on Personal Data using any electronic means, including processing and other means. This processing includes collecting, storing, recording, organizing, adapting, modifying, circulating, altering, retrieving, exchanging, sharing, using, characterizing, disclosing Personal Data by broadcasting, transmitting, distributing, making available, coordinating, merging, restricting, blocking, erasing or destroying it or creating forms thereof |
| **Automated Processing** | : | Processing which is carried out using an electronic program or system which operates in an automated and automatic manner either completely independently without any human intervention or partially with limited human supervision and intervention |
| **Personal Data Security** | : | A set of technical and organizational measures, procedures and processes specified in accordance with provisions of this Decree by Law which maintain the protection of privacy, confidentiality, integrity and availability of Personal Data |
| **Pseudonymisation** | : | Processing performed on Personal Data in such a way which, after the completion of processing, makes it not possible to associate and attribute such data to the Data Subject without the use of additional information, provided that such additional information |

| | | |
|---|---|---|
| | | is kept independently and securely. In accordance with the technical and organizational measures and procedures specified under provisions of this Decree by Law, it shall ensure that Personal Data is not linked to a specific natural person or that he/she can be identified by using it |
| **Anonymization** | : | Processing which is performed on Personal Data in a way which leads to the anonymity of the Data Subject, not linking and attributing such data to him/her and the inability to identify him/her in any way whatsoever |
| **Data Breach** | : | Breaching information security and Personal Data through illegal or unauthorized access. This includes copying, sending, distributing, exchanging, transferring, circulating or processing it in a way which leads to disclosure of such data to third parties, or destroying or modifying it during storage, transfer and processing |
| **Profiling** | : | A form of automated processing which involves the use of Personal Data to assess certain personality aspects associated with the Data Subject, including analyzing or predicting aspects related to his/her financial performance or condition, health, personal preferences, interests, behavior, location, movements or reliability |
| **Cross-Border Processing** | : | Dissemination, use, display, transmission, reception, retrieval, sharing or processing of Personal Data outside the State |
| **Consent** | : | The consent whereby the Data Subject authorizes a third party to process his/her Personal Data, provided that this consent |

indicates, in a specific, clear and unambiguous manner, that he/she accepts the processing of his/her Personal Data through a clear positive statement or action

## Article (2)

## Scope of Application of the Decree by Law

1. Provisions of this Decree by Law shall apply to the processing of all or part of the Personal Data by means of electronic systems which operate automatically, or by other means, by the following:
   a. Each Data Subject residing in the State or having a place of business in it.
   b. Each Controller or Processor residing in the State and carrying out the activities of processing Personal Data of Data Subjects inside and outside the State.
   c. Each Controller or Processor residing outside the State and carrying out the activities of processing Personal Data of Data Subjects inside the State.
2. Provisions of this Decree by Law shall not apply to the following:
   a. Government Data
   b. Governmental entities which control or process Personal Data.
   c. Personal Data held by the security and judicial authorities
   d. A Data Subject who processes his/her data for personal purposes.
   e. Personal Health Data that has legislation regulating its protection and processing.
   f. Personal banking and credit data and information that have legislation regulating their protection and processing.
   g. Companies and establishments located in free zones in the Country and have special

legislations regarding Personal Data protection.

## Article (3)

## Bureau's Power of Exemption

Without prejudice to any other competencies prescribes for the Bureau under any other legislation, the Bureau may exempt some establishments that do not process a large volume of Personal Data from part, or all of the requirements of the personal data protection provisions stipulated in this Decree by Law, in accordance with the standards and controls set by the Executive Regulations of this Decree by Law.

## Article (4)

## Cases of Processing Personal Data without the Consent of its Owner

It is prohibited to process Personal Data without the consent of its owner. The following cases shall be excluded from such prohibition:

1. If the processing is necessary to protect public interest.
2. If the processing is related to Personal Data which has become available and known to all by an act of the Data Subject.
3. If the processing is necessary to initiate any procedures of legal claim or defense of rights or is related to judicial or security procedures.
4. If the processing is necessary for purposes of occupational or preventive medicine in order to assess the employees' ability of to work, performing medical diagnosis, providing health or social care, treatment or health insurance services, managing 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 protection from existing diseases and epidemics, or for the purposes of ensuring the safety and quality of healthcare, 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 purposes of the Controller or Data Subject carrying out their obligations and exercising their legally established rights in the field of employment, social security or laws concerned with social protection, to the extent permitted by such Laws.
9. If the processing is necessary to perform a contract to which the Data Subject is a party, or to take measures at the request of the Data Subject with the aim of concluding, amending or terminating a contract.
10. If the processing is necessary to fulfil specific obligations stipulated in other laws in force in the State for the Controller.
11. Any other cases set out in the Executive Regulations of this Decree by Law.

## Article (5)

## Personal Data Processing Controls

Personal Data shall be processed according to the following controls:

1. Processing shall be carried out in a fair, transparent and lawful manner.
2. Personal Data shall be collected for a specific and clear purpose. It shall not be processed at

any later time in a manner incompatible with such purpose. However, it may be processed if the purpose is similar or close to the purpose for which this data is collected.

3. Personal Data shall be sufficient and limited to what is necessary in accordance with the purpose for which the processing is carried out.
4. Personal Data shall be accurate and correct and shall be updated whenever necessary.
5. The necessary measures shall be taken to ensure that incorrect Personal Data is deleted or corrected.
6. Personal Data shall be kept securely, including protecting it from any violation, penetration, or illegal or unauthorized processing through the development and use of appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard.
7. Personal Data shall not be kept after the purpose of its processing has been exhausted. It may be kept if the identity of the Data Subject has been concealed using the "Anonymization Mechanism"
8. Any other controls set out in the Executive Regulations of this Decree by Law.

## Article (6)

## Terms of Consent to Data Processing

1. To be considered, the consent of the Data Subject to the processing of date shall require the following:
    a. The Controller shall be able to prove the consent of the Data Subject in the event that the processing of Personal Data is based on the consent of the Data Subject.
    b. The Consent shall be prepared in a clear, simple, unambiguous and easily accessible

manner, whether in writing or electronically.

c. The Consent shall include the Data Subject's right to withdraw it easily.

2. The Data Subject may, at any time, withdraw their consent to the processing of Personal Data. Such withdrawal of consent shall not affect the legality of the processing based on the given consent before withdrawing it.

## Article (7)

## The Controller's General Obligations

The Controller shall abide by the following:

1. Take appropriate technical and organizational measures to implement the necessary standards to protect and secure Personal Data in order to preserve its confidentiality and privacy, and to ensure that it is not breached, destroyed, altered or tampered with, taking into account the nature, scope and purposes of processing and the possibility of risks to the confidentiality and privacy of the Data Subject's Personal Data.
2. Apply the appropriate measures, whether while determining the means of processing or while processing, in order to comply with the provisions of this Decree by Law, including the controls stipulated in Article (5). These measures include the Pseudonymisation Mechanism.
3. Apply appropriate technical and organizational measures with respect to automatic settings, to ensure that the processing of Personal Data is limited to the purpose for which it is intended. Such obligation shall apply to the volume and type of Personal Data collected, the type of processing which will be carried out, the period of storage and accessibility of such data.

4. Maintain a special record for Personal Data, provided that such record shall include the data of both the Controller and the Data Protection Officer, a description of the categories of Personal Data, details of the persons authorized to access the Personal Data, processing times, limitations and scope, the mechanism for erasing, modifying or processing Personal Data, the purpose of processing, any data related to the cross-border movement and processing of such data, and the technical and organizational measures related to information security and processing The Controller shall submit such record to the Bureau whenever requested to do so.
5. Appoint the Processor which has sufficient guarantees to implement technical and organizational measures in a manner which ensures that the processing meets the processing requirements, rules and controls stipulated in this Decree by Law, its Executive Regulations and the decisions issued to implement the same.
6. Provide the Bureau, pursuant to a decision made by the competent judicial authority, with any information it requests in implementation of its powers stipulated in this Decree by Law and its Executive Regulations.
7. Any other obligations set out in the Executive Regulations of this Decree by Law.

## Article (8)

## The Processor's General Obligations

The Processor shall abide by the following:

1. Carry out the processing in accordance with the instructions of the Controller and contracts and agreements concluded between them, which specify in particular the scope, subject, purpose, nature and type of Personal Data, and the category of the Data Subject.

2. Apply the appropriate technical and organizational procedures and measures to protect Personal Data at the design stage, whether during the identification of the means of processing or during the processing, taking into account the cost of implementing such procedures and the nature, scope and purposes of processing.
3. Carry out the processing according to the purpose and the period specified for it. If the processing exceeds the specified period, the Processor shall so notify the Controller to authorize it to extend such period or give appropriate instructions.
4. Erase data after the expiry of the processing period or upon handing it over to the Controller.
5. Avoid doing anything which would disclose Personal Data or results of processing, except in cases authorized by the law.
6. Protect and secure data processing, the electronic media and devices used in processing and the Personal Data they contain.
7. Maintain a special record of Personal Data which is processed on behalf of the Controller, provided that such record includes the data of the Controller, the Processor and the Data Protection Officer and a description of the categories of Personal Data they have, data of the persons authorized to access Personal Data, processing times, restrictions and scope, the mechanism of erasing, modifying or processing Personal Data, the purpose of processing, any data related to the cross-border movement and processing of such data and the technical and organizational measures related to information security and processing operations, provided that the Processor submits such record to the Bureau whenever it is requested to do so.
8. Provide all means to prove its commitment to the implementation of provisions of this Decree by Law when so requested by the Controller or the Bureau.

9. Carry out processing in accordance with rules, conditions and controls specified in this Decree by Law and its Executive Regulations, or pursuant to which instructions are issued by the Bureau.
10. In the event that more than one Processor participates in processing data, the processing shall be carried out in accordance with a written contract or agreement in which they clearly define their obligations, responsibilities and roles with regard to processing, otherwise they shall be deemed jointly responsible for the obligations and responsibilities contained in this Decree by Law and its Executive Regulations.
11. The Executive Regulations of this Decree by Law shall specify the procedures, controls, conditions, and technical standards related to such obligations.

## Article (9)

## Reporting Personal Data Breach

1. In addition to the obligations of the Controller stipulated in this Decree by Law, the Controller shall, at the time it becomes aware of the existence of any breach or violation of Personal Data of the Data Subject that would prejudice the privacy, confidentiality and security of data, notify the Bureau of such breach or violation and the investigation rights within the period and in accordance with the measures and requirements set by the Executive Regulations of this Decree by Law, provided that the reporting is accompanied by the following data and documents:
    a. A description of the nature of the breach or violation, its form, causes, approximate number and records.
    b. Details of the appointed Data Protection Officer.

c. Potential and expected effects of the breach or violation.

d. Corrective measures and actions taken or suggested by it to confront such violation and reduce its negative impacts.

e. Documents of the violation and corrective actions taken by it.

f. Any other requirements required by the Bureau

2. In all cases, the Controller shall notify the Data Subject in the event that the violation or breach would prejudice the privacy and confidentiality of the security of his/her Personal Data within the period and in accordance with the measures and requirements set by the Executive Regulations of this Decree by Law. It shall inform him/her of the measures taken by it.
3. If the Processor becomes aware of any breach of Personal Data, it shall notify the Controller of such breach as soon as it becomes aware of the same. the Controller shall in turn inform the Bureau in accordance with Clause (1) of this Article.
4. After receiving the notification from the Controller, the Bureau shall verify the reasons for the violation to ensure the integrity of the security measures taken, and impose the administrative penalties referred to in Article (26) of this Decree by Law in the event that a violation of its provisions and decisions issued in implementation of it is proven against the Controller or the Processor.

## Article (10)

## Appointing Data Protection Officer

1. The Controller and Processor shall appoint a Data Protection Officer, who has sufficient skills and knowledge of the Personal Data Protection Law, in any of the following cases:

a. If 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 new technologies or with regard to the volume of data.
b. If processing would involve a systematic and comprehensive assessment of Sensitive Personal Data, including Profiling and Automated Processing.
c. If processing would be carried out on a large volume of Sensitive Personal Data.

2. The Data Protection Officer may be an employer of the Controller or the Processor or authorized by them, whether inside or outside the State.
3. The Controller or the Processor shall specify the contact details of the Data Protection Officer and notify the Bureau of the same.
4. The Executive Regulations of this Decree by Law shall specify the types of technologies and criteria for determining the volume of data required in accordance with this Article.

## Article (11)

## Roles of Data Protection Officer

1. The Data Protection Officer shall ensure the extent of compliance of the Controller or the Processor with the application of provisions of this Decree by Law, its Executive Regulations and instructions issued by the Bureau. The Data Protection Officer shall, in particular, undertake the following tasks and powers:
   b. Verifying the quality and correctness of the procedures in place at the Controller and the Processor.
   b. Receiving requests and complaints related to Personal Data in accordance with provisions of this Decree-Law and its Executive Regulations.

c. Providing technical advice on evaluation procedures and periodic examination of personal data protection systems and intrusion prevention systems at 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 link between the Controller or the Processor, as the case may be, and the Bureau regarding the application of personal data processing provisions stipulated in this Decree by Law.
e. Any other tasks or powers which are determined in accordance with the Executive Regulations of this Decree by Law.

2. The Data Protection Officer shall maintain the confidentiality of information and data it receives in implementation of its duties and powers in accordance with provisions of this Decree by Law and its Executive Regulations and in accordance with the legislations in force in the State.

## Article (12)

## Duties of the controller and the processor towards the Data Protection Officer

1. The Controller and the Processor shall provide all means to ensure that the Data Protection Officer performs the duties and tasks assigned to it as stipulated in Article (11) of this Decree by Law in the required manner. In particular, this shall include the following:
   a. Ensure that the Data Protection Officer is appropriately and timely involved in all matters relating to the protection of Personal Data.
   b. Ensure that the Data Protection Officer is provided with all the necessary resources and the necessary support to carry out the tasks assigned to it.

c. Not to terminate the Data Protection Officer services or impose any disciplinary penalty for a reason related to the performance of its duties in accordance with the provisions of this Decree by Law.

d. Ensure that the Data Protection Officer is not charged with duties which contradict its duties under this Law.

2. The Data Subject may communicate directly with the Data Protection Officer about all matters relating to his/ her personal data processing to enable him/ her to exercise his/ her rights in accordance with the provisions of this Decree by Law.

## Article (13)

## Right to Receive Information

1. The Data Subject has the right, by submitting a request to the Controller without any consideration, to obtain the following information:

   a. The types of its Personal Data that are being processed.

   b. Purposes of processing.

   c. Decisions made based on automated processing, including profiling.

   d. The targeted sectors or establishments with whom its personal data will be shared from inside and outside the State.

   e. Controls and standards for the period of storage and preservation of his/ her personal data.

   f. Procedures for correcting, erasing or limiting processing and objection to his/ her personal data.

   g. Protection measures for cross-border processing carried out in accordance with Articles

(22) and (23) of this By-Law.

h. Actions to be taken in the event of a breach or misuse of his/ her Personal Data, especially if the breach or misuse has a direct and serious threat to the privacy and confidentiality of his/her Personal Data.

i. How to submit complaints to the Bureau.

2. In all cases, the Controller shall, before starting the processing, provide the Data Subject with the information stipulated in paragraphs (b), (d) and (g) of Paragraph (1) of this Article.

3. The Controller may reject the Data Subject's request to obtain the information mentioned in Paragraph (1) of this Article, if the following is established:

   a. The request is not related to the information referred to in Paragraph (1) of this Article, or it is excessively repetitive.

   b. The request conflicts with judicial procedures or investigations conducted by competent authorities.

   c. The request may negatively affect the efforts of the Controller to protect information security.

   d. The request affects the privacy and confidentiality of Personal Data of third parties.

## Article (14)

## Right to Request Transfer of Personal Data

1. The Data Subject shall have the right to receive his/her personal data that has been provided to the Controller for processing, in an orderly and machine-readable manner, whenever the processing is based on the consent of the Data Subject, or it is necessary for the implementation of a contractual obligation, and it is carried out by automated means.

2. The Data Subject shall have the right to request the transfer of its Personal data to another Controller whenever it is technically feasible.

## Article (15)

## Right to correction or erasure of Personal Data

1. The Data Subject shall have the right to request the correction of his/her inaccurate Personal data, or request to complete the data held by the Controller without undue delay
2. Without prejudice to the legislations in force in the State and what is required for the public interest, the Data Subject shall have the right to request erasure of his/ her Personal Data held by the Controller in any of the following cases:
    a. His/her Personal Data is no longer necessary for the purposes for which it is collected or processed.
    b. Withdrawal of the consent of Data Subject on which the processing is based.
    c. The Data Subject's objection to the processing, or the absence of legitimate reasons for the Controller to continue the processing.
    d. The Personal Data is processed in violation of the provisions of this Decree by Law and the applicable legislations, and the erasure process is necessary to comply with the legislations and approved standards in force in this regard.
3. As an exception to what is stated in Paragraph (2) of this Article, the Data Subject is not entitled to request erasure of his/ her Personal Data held by the Controller in the following cases:
    a. If the request is related to the erasure of his/her Personal Data related to public health in private facilities.

b. If the request affects the investigation procedures and claiming and defending rights.

c. If the request contradicts other legislations to which the Controller is subject.

d. Any other cases determined by the Executive Regulation of this Decree by Law.

## Article (16)

## Right to Restrict Processing

1. The Data Subject shall have the right to oblige the Controller to restrict and stop processing in any of the following cases:
   a. The Data Subject's objection to the accuracy of the Personal Data, in which case the processing shall be restricted for a specific period to allow the Controller to verify the data accuracy.
   b. The Data Subject's objection to the processing of his/ her Personal Data in violation of the agreed-upon purposes.
   c. The processing is carried out in violation of the provisions of this Decree by Law and the applicable legislations.
2. The Data Subject shall have the right to request the Controller to continue to keep his/ her Personal Data after the completion of the processing purposes when such data is necessary to complete procedures related to claiming or defending rights and lawsuits.
3. Notwithstanding what is stated in Paragraph (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 pursue any of the procedures related to claiming or

defending rights and lawsuits or related to judicial proceedings.

c. If the processing is necessary to protect the rights of third parties.

d. If the processing is necessary to protect the public interest.

4. In all cases, the Controller, if it lifts the restriction stipulated in this Article, shall notify the Data Subject of the same.

## Article (17)

## Right to Stop Processing

The Data Subject shall have the right to object to the processing of his/her Personal Data and stop it in any of the following cases:

1. If the processing is intended for the purposes of direct marketing, including profiling related to direct marketing.
2. If the processing is intended for the purposes of conducting statistical surveys, unless the processing is necessary to serve the public interest.
3. If the processing is carried out in violation of Article (5) of this Decree by Law.

## Article (18)

## Right to Processing and Automated Processing

1. The Data Subject shall have the right to object to any decisions resulting from automated processing, including profiling, particularly those decisions which have legal impact on or adversely affect the Data Subject.
2. Notwithstanding Paragraph 1 of this Article, the Data Subject may not object to the decisions resulting from automated processing in the following cases:

a. If the automated processing is agreed upon under the contract made between the Data Subject and the Controller.
b. If the automated processing is required under other legislations which are applicable in the State.
c. If the Data Subject gives prior consent to the automated processing as set out in Article (6) of this Decree by Law.

3. The Controller shall adopt appropriate measures to protect the privacy and confidentiality of the Data Subject's Personal Data in the cases referred to in Paragraph 2 of this article and shall not cause any prejudice to the Data Subject's rights.
4. The Controller shall include the human element in reviewing automated processing decisions at the request of the Data Subject.

## Article (19)

## Contacting the Controller

The Controller shall provide clear and appropriate ways for the Data Subject to contact the Controller to request any of the rights set forth in this Decree by Law.

## Article (20)

## Personal Data Security

1. The Controller and the Processor shall develop and take appropriate technical and regulatory measures to ensure the highest standard of information security that is suitable for the risks related to data processing in accordance with the best international practices and standards. This shall include the following:

a. Encryption of Personal Data and the application of Pseudonymisation.
b. Applying measures which ensure the continuous confidentiality, safety, accuracy and flexibility of data processing systems and services.
c. Applying measures which ensure timely retrieval of and access to Personal Data in case of any actual or technical failure.
d. Applying measures which ensure a seamless testing and evaluation of the effectiveness of the technical and regulatory measures to ensure the security of processing.

2. When evaluating the information security level as set out in Paragraph1 of this Article, the following shall be observed:
   a. Data processing risks, including damage, loss, accidental or illegal change and disclosure of or access to the Personal Data, whether being transferred, stored or processing.
   b. The costs of data processing, and its nature, scope and purposes, in addition to potential risks impacting the confidentiality and privacy of the Data Subject's Personal Data.

## Article 21

## Assessment of the Impact of Personal Data Protection

1. Taking into account the nature, scope and purposes of data processing, the Controller shall, before carrying out the processing, evaluate the impact of the proposed processing operations on the protection of Personal Data, when using any of the modern technologies that would pose a high risk to the privacy and confidentiality of the Data Subject's Personal Data.
2. The assessment of the impact provided for in Paragraph (1) of this Article shall be required in the following cases:

a. If the processing includes a systematic and comprehensive assessment of the personal aspects of the Data Subject, using automated processing, including profiling, having legal consequences or serious impact on the Data Subject.
b. If processing would be carried out on a large volume of Sensitive Personal Data.

3. The assessment stipulated in Paragraph (1) of this Article shall include, at a minimum, the following:
   a. Clear and systematic explanation of the suggested processing operations for the protection of Personal Data and the purpose of processing.
   b. Evaluation of how necessary the processing operations are and how they are suitable for the purpose of processing.
   c. Evaluation of potential risks related to the privacy and confidentiality of the Data Subject's Personal Data.
   d. The suggested procedures and measures aimed at reducing the potential risks related to the protection of Personal Data.
4. The Controller may carry out one evaluation of a set of processing operations which have similar nature and risks.
5. The Controller shall coordinate with the Data Protection Officer upon evaluating the impact of the protection of Personal Data.
6. The Bureau shall prepare a list of processing operation types which do not require evaluation of the impact of the protection of Personal Data. The Bureau shall publish such list on its website.
7. The Controller shall review the evaluation results on a regular basis to make sure that the processing is being carried out in accordance with the evaluation in case the processing risks

level changes.

## Article (22)

## Cross-Border Transfer and Sharing of Personal Data for Processing Purposes if a Proper Protection Level is Available

Personal Data may be transferred to outside of the State in the following cases approved by the Bureau:

1. The State or Province to which the Personal Data is transferred shall have legislations addressing Personal Data Protection. This includes most significant provisions, measures, controls, stipulations and rules related to the protection of the privacy and confidentiality of the Date Subject's Personal Data, and his/her ability to exercise their legal rights. The State or the Province shall also have a judicial o regulatory authority imposing appropriate measures against the Controller or the Processor.
2. If the State joins a bilateral or multilateral agreement related to the protection of Personal Data concluded with countries to which the Personal Data is transferred.

## Article (23)

## Cross-Border Transfer and Sharing of Personal Data for Processing Purposes if a Proper Protection Level is not Available

1. Notwithstanding Article (22) of this Decree by Law, Personal Data may be transferred to outside the State in the following cases:
    a. Companies, operating in countries where there are no laws for Data Protection, may transfer data under a contract or agreement obligating the companies in such countries

to adopt measures, controls and requirements set out in this Decree by Law, in addition to provisions forcing the Controller or the Processor to adopt appropriate measures which are imposed by a judicial or regulatory authority in such countries as set out in the contract.

b. If there is an explicit consent granted by the Data Subject to transfer his/her Personal Data outside the State, provided that such transfer shall not contradict the public or security interest of the State.
c. If the transfer is necessary to fulfil obligations and establish rights before judicial entities, exercise or defend the same.
d. If the transfer is necessary to sign or implement a contract made between the Controller and the Data Subject, or between the Controller and third parties to serve the interest of the Data Subject.
e. If the transfer is necessary to implement an action related to an international judicial cooperation.
f. If the transfer is necessary to protect the public interest.

2. The Executive Regulations of this Decree by Law set forth the controls and stipulations referred to in Paragraphs (1) of this Article, which should be observed during the transfer of data outside the State.

## Article (24)

## Complaints

1. The Data Subject shall have the right to submit complaints to the Bureau if he/she believes that there is a violation of this Decree by Law or that the Controller or the Processor is

processing his/ her Personal Data in violation of the rules and procedures set by the Bureau in this regard.

2. The Bureau shall receive complaints from the Data Subject in accordance with Paragraph (1) of this Article and shall examine such complaints in coordination with the Controller and the Processor.
3. The Bureau shall impose the administrative penalties referred to in Article (26) of this Decree by Law if it is proven that the Controller or the Processor violates its provisions, or the decisions issued in implementation of the same.

## Article (25)

## Grievance against the Bureau's Decisions

Any stakeholder may submit a written grievance to the General Director of the Bureau against any decision or administrative penalty or any other action taken by the Bureau against such stakeholder within (30) thirty days as of the date on which a notice of such administrative decision or penalty is given. Additionally, deciding upon such complaint shall be made within (30) thirty days as of the date on which the complaint is submitted.

It is not permissible to challenge any decision issued by the Bureau in implementation of the provisions of this Decree by Law before submitting a grievance against the same. The Executive Regulations of this Decree by Law set out the procedures for submitting a grievance and deciding thereupon.

## Article (26)

## Administrative Penalties

The Council of Ministers, based upon a suggestion from the General Director of the Bureau, shall issue a decision to limit the actions which constitute a violation of this Decree by Law and its Executive Regulations, including administrative penalties to be imposed.

## Article (27)

## Authorization

The Council of Ministers, based upon a suggestion from the General Director of the Bureau, may authorize any competent local government authority within the scope of its local competence, to exercise some of the Bureau' powers set out in this Decree by Law.

## Article (28)

## The Executive Regulation

The Council of Ministers, based upon a suggestion from the General Director of the Bureau, shall issue the Executive Regulations of this Decree by Law within six (6) months as of the date on which the Decree by Law is promulgated.

## Article (29)

## Regularisation

The Controller and the Processor shall regularize their status in compliance with the provisions of this Decree by Law within a period of no more than six (6) months as of the date on which its Executive Regulations are issued. The Council of Ministers may extend such period for another similar period.

## Article (30)

## Repeals

Any provision that violates or contradicts the provisions of this Decree by Law shall be repealed.

## Article (31)

## Publication & Enforcement of this Decree by Law

This Decree by Law shall by published in the Official Gazette and shall come into force as of 02 January 2022.

**Khalifa Bin Zayed Al-Nahyan**

**President of the United Arab Emirates**

Issued by us at the Presidency Palace in Abu Dhabi:
On: 13 / Safar / 1443 AH
Corresponding: 20 / September / 2021AD