Preamble

First, at present, there is no single Act specifically addressing the "Subject Issue" (i.e. Protection of Personal Data).

However, the Bill of Preservation and Protection of Personal Data dated 06/05/1397 (28/07/2018) (the "**PPPD**") has been submitted by the Ministry of Information and Communications Technology (the "MICT") and is yet under review by the Islamic Consultative Assembly of Iran (the "Parliament").

In addition, the Subject Issue has been somehow addressed in different laws and regulations, more particularly, in Principle 25 of the Constitution of Islamic Republic of Iran as well as other Iranian legislations including Law on Publication and Free Access to Data (2009) (the "**PFAD**") and its subsequent regulations, Law on Duties and Powers of MICT (2003), Law on Electronic Commerce (2004), Islamic Penal Code (1996), Criminal Procedure Code (2014), the Amendment to Anti-Money Laundering Law (2019) and its subsequent regulation (2020).

Finally, a reference to prohibition of disclosure of client's secrets is made in some regulations for specific professions, such as the Regulation of the Bill on the Independence of the Bar Association applicable for lawyers and Disciplinary Regulation of Violations by Guilds and Professional Unions of Medical and related Professions.

In conclusion, excluding the PPPD and PFAD, the foregoing laws and regulations address the Subject Issue for specific cases providing one or a few articles in this regard. For instance, Article 64 of Electronic Commerce Act imposes fines for illegal acquisition of trade or economic secrets of agencies and institutions or the disclosure of such secrets to third parties in electronic environment, or Article 731 of Islamic Penal Code imposes punishment for any person who, without authorization, commits acts in connection with secret data being transmitted or stored on computer or telecommunication platform or data carrying systems, or Article 648 of the latter law which provides punishment for disclosure of client's secrets by specific professionals including doctors, pharmacists etc.

Jurisdiction	Islamic Republic of Iran
Date	April 5, 2022
Law Firm	Torossian, Avanessian and Associates
Title, Name	V. Torossian (Partner) Shaghig Abedi (Associate)
Contact Information	Address: 17 Magnolia St., Golriz St., Ghaem Magham Farahani Ave., Tehran, Iran Email: v.torossian@taalawfirm.com s.abedi@taalawfirm.com Tel: (021) 88 84 28 43, 88 84 31 39, 88 84 31 40

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future? **Please refer to the preamble, more particularly the PFAD (at the present) and PPPD (in the future).**

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future? **Please refer to the preamble, more particularly the PFAD (at the present) and PPPD (in the future).**

iii. Does your country have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.) **Please refer to the preamble.**

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law ：**PPPD (Bill) – Public and Private Sector**

① The definition of "Personal Information"	**Article (2):** **Paragraph (A): Personal Data: is data that, by itself or in combination with other data, directly or indirectly, identifies the subject of the data, by referring to an identifier.** **Paragraph (B) : Sensitive Personal Data: is personal data that reveals ethnic or tribal origins, political, religious and philosophical views, hereditary characteristics or health information of the subject person of the data.**
② The scope in which the law applies	**Article (3): The subject persons of the law are:** **(A) : Natural person or legal entity being an Iranian citizen, public or private, whether their personal data is processed inside or outside Iran.** **(B) Foreign natural person or legal entity, public or private, whose personal data is processed by an Iranian controller or processor.**
③ The territorial scope	**There is no specific provision regulating the territorial scope of application.**

The title of the law ：**PFAD (Law) - Public and Private Sector**

① The definition of "Personal Information"	**Article (1):** **Paragraph (B) : Personal Information: information pertaining to individuals such as name, surname, home and work addresses, the situation of family life, personal habits, physical problems, bank account number and password.**
② The scope in which the law applies	**There is no specific provision regulating the scope in which the law applies.**
③ The territorial scope	**There is no specific provision regulating the territorial scope of application.**

ii. If there are any special instructions about the laws, please describe them.
The special instructions are addressed in the Implementing Regulations of PFAD.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Kindly note, considering that, at present, there is no unified law or regulation which embodies OECD Privacy Principle in Iran and that, in general, such principles can be found in a scattered manner in different laws, therefore, we will respond to the inquiry of this section, by providing you with some law provisions for each principle, as an example, as follows:

(a) Collection Limitation Principle

Articles 14, 15 and 16 of PFAD as follows:

Article 14 – If the requested information pertains to privacy of persons, or is regarded as information obtained through the violation of privacy of subject person, the request should be rejected.

Article 15 – If accepting the request leads to the illegal disclosure of personal information of the third person, the institutions subject to this law (i.e. public and private sectors) should withhold the requested information unless:

A – The third party has given his/her consent, explicitly and in writing, to the disclosure of information about him/her.
B – The applicant is the third party's legal guardian or lawyer, and acting within his/her powers.
C – The applicant is a public institution, and the requested information is, based on the law, directly related to its powers and duties.

Article 16 – If, based on legal evidences, it is proven to the institutions subject to this law that providing the requested information will jeopardize individuals' life or health or inflict material or trade losses upon them, the institutions should

withhold the information.

(b) Data Quality Principle

As we understand from the content of the Data Quality Principle described in OECD Guidelines, to the best of our knowledge there is no Iranian law provision in this regard.

(c) Purpose Specification Principle

Article 8 of Anti-Money Laundering Law provides *"The information and documents collected for the purpose of implementing this Law will be used solely in connection with the objectives as mentioned in the present Law as well as for combating its predicate offences. Disclosure or use of the information, directly or indirectly, whether by government officials or others, for their own benefit or third parties, is prohibited and the offender will be punished…"*

(d) Use Limitation Principle

Article 15 of PFAD as described in paragraph (a) above.
Article 8 of Anti-Money Laundering Law described in paragraph (c) above.

(e) Security Safeguards Principle

Article 669 of Criminal Procedure Code which provides that whenever the preservation of stored computer data is necessary for an investigation or a trial, a judicial authority may order the protection of such information for those persons who are in possession or control of such information. In urgent circumstances, such as the risk of injury or loss or alteration of data, judicial officers may issue a protection order and notify the judicial authority within a maximum of twenty-four hours. If any of government employees or judicial officers or other persons refuses to comply with such order or disclose the protected data, or inform the persons to whom the data relates of the provisions of such order, the offender shall be subject to the punishment provided by law.

Article 8 of Anti-Money Laundering Law provides *"… Disclosure or use of the information, directly or indirectly, whether by government officials or others, for their own benefit or third parties, is prohibited and the offender will be punished…"*

(f) Openness Principle

As we understand from the content of the Openness Principle described in OECD Guidelines, to the best of our knowledge there is no general policy of openness about developments, practices and policies with respect to personal data.

(g) Individual Participation Principle

Articles 6, 7, 8 and 9 of PFAD as follows:

Article 6 – Requests for access to private information shall only be accepted from natural persons to whom the information is related, or from their legal representatives.

Article 7 – A public institution is not authorized to ask applicants requesting information to provide a reason or justification for their request.

Article 8 – A public or private institution should reply to the request for information as soon as possible, and the time to reply should not exceed maximum ten days after the request is received. In six months' time from the date this law is ratified, the Implementing Regulation on the enforcement of this article shall be proposed … and approved … *(the aforesaid Implementing Regulation is already enacted in June 13, 2021)*

Article 9 – Replies by private institutions to the requests for access to information should be in writing or electronic.

(h) Accountability Principle

As we understand from the content of the Accountability Principle described in OECD Guidelines as well as the fact that there is no unified law regarding the OECD principles, to the best of our knowledge there is no specific data controller who should be accountable for complying with measures which give effect to such principles.

However, in each specific law, an authority who is liable for controlling the due implementation of the law might be appointed. For instance, Article 18 of PFAD provides that *"In order to support freedom of information and public access to the information available at public and private institutions which offer public services, the Commission on Dissemination of and Free Access to Information shall be established… in order to draw up executive plans required for information dissemination, monitor the proper implementation of the plans, settle the disputes on how to provide information by standard practice making , promote the culture of freedom of information and offer guidelines as well as consultative opinions…".*

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

With regard to possible exclusion of each OECD Privacy Principle, the provisions of law are even more scattered. Therefore, we kindly draw your attention to below (3) examples of law, merely for giving you a picture of local law provisions which might be considered as an exclusion of OECD Privacy Principle:

(1) Article 13 of PFAD provides *"In the event that the applicant's request is related to classified documents and information (state secrets), public institutions should withhold such information. Access to classified information is subject to specific laws and regulations."*

(2) Article 17 of PFAD provides *"The institutions subject to this law are obliged to withhold information in cases where the requested information shall harm or disrupt the following:*

a – Public peace and security;
b – Prevention or investigation of crimes or prosecution of criminals;
c – Auditing and collecting taxes or legal levies/charges;
d – Monitoring immigration into the country.

Note 1 – The provisions of Articles 13 to 17 *(as described in this Section and (III) (i) (a) above)* ***shall not apply to information regarding the existence or emergence of environmental risks and threats to public health.***

Note 2 – The subject of Articles 15 and 16 *(as described in (III) (i) (a) above)* ***shall not apply to information which might lead to defamation, outrage public decency or promote obscene acts."***

(3) Article 14 of Countering the Financing of Terrorism Act which provides *"All persons covered by the Anti-Money Laundering Law are required to submit a report on suspected terrorist financing operations to … . Persons who attempt to send reports to the relevant authorities in accordance with this Article shall not be subject to penalties related to the disclosure of personal secrets"*

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

To the best of our knowledge, none.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

The Ministry of Information and Communications Technology as well as the Commission on Dissemination of and Free Access to Information as described in (III)(i)(h) above.