

DATA PROTECTION LAWS OF THE WORLD

Iran



Downloaded: 12 May 2024

IRAN



Last modified 23 May 2019

LAW

Iran has not enacted comprehensive data protection legislation. However, several laws and regulations incorporate data protection provisions.

These include:

- Sharia law principles
- The Constitution of the Islamic Republic of Iran
- Draft of the Bill on Protection of Data and Privacy in the Cyber Space 2018
- Charter of Citizen's Rights 2016
- Cyber Crime Act 2011
- The Law Concerning Protection of Consumers Rights 2010
- The Law on Publishing and Access to Data 2010
- Stock Market Law 2006
- Electronic Commerce Law (ECL 2004)
- The Law on Facilitation of Competition and Prevention of Monopoly 2004
- The Law on respect for Legitimate Rights and Citizen Rights 2004
- The Law on Establishment of the Ministry of Justice Official Experts 2003
- Press Law 2001
- Criminal Code 1997
- Bylaw Concerning Official Translators 1996
- Criminal Procedures Code 1994
- Direct Taxation Act as amended 1988
- The Law on Statistic Centre of Iran 1976
- Civil Liability Code 1960
- The Law on Establishment of Notary Public Offices 1937
- Iranian Bar Association Law 1936

DEFINITIONS

Definition of Personal Data

Not specifically defined.

Under the Law on Publishing and Access to Data, "personal data" means first and last name, home and work address, individual habits, bank accounts information, etc.

The E-Commerce Law defines "private data" as a "data message" associated with a specific data subject. "Data message" means any representation of facts, information, and concepts generated, sent, received, stored or processed by use of electronic, optical or other information technology means.

Definition of Sensitive Personal Data

Not specifically defined.

Under the E-Commerce Law "sensitive personal data" has customarily been understood to mean data relating to family matters, criminal records, tribal or ethnic origins, moral and religious beliefs, ethical characteristics, sexual habits and data regarding health, physical or psychological status.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Iran.

REGISTRATION

There is no registration requirement.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Data collection and processing, including publication, is subject to data subject consent, provided that the "data message" is otherwise in accordance with Iranian law.

The collection and processing of personal "data messages" via electronic means is subject to the following conditions:

- the purpose of collection and processing must be specified and clearly described
- data may only be collected to the extent necessary to achieve its purported purpose
- "data messages" must be correct and up-to-date
- data subjects must be provided with access to computer files that contain "data messages" that concern the data subject
- data subjects must be provided with the ability to delete or rectify "data messages" in accordance with relevant regulations (Article 59, E-Commerce Law)

Unless otherwise provided by law, the following is prohibited: searching, collecting, processing, using or disclosing personal data. This prohibition also applies to other mail and telecommunications, including telephone communications, faxes, wireless and private internet communications.

TRANSFER

The Charter of Citizen's Rights prohibits personal data transfers without express data subject consent.

Under the ECL, third party and extraterritorial data transfers are subject to:

- data subject consent
- assurance that adequate security levels are in place to protect personal data in accordance with data subject rights and freedoms

SECURITY

Generally, Iranian business are required to take reasonable measures to secure personal information. It is unclear whether such measures must be physical, technical or organizational.

Nevertheless, somehow effective regulations apply to some businesses which are involved in sensitive information such as judges, attorneys, doctors, hospitals and pharmacies.

Under the ECL, **secure information system** is defined as an information system that:

- is reasonably protected against misuse or penetration
- possesses a reasonable level of proper accessibility and administration
- is reasonably designed and organized in accordance with the significance of the task
- is in compliance with secure methods

A **secure method** is a method to authenticate **data message**; date, correctness, origin and destination, as well as to detect errors and modifications in its communication, content, or storage from a certain point. A secure message is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures or similar secure techniques.

BREACH NOTIFICATION

There is no requirement to report data breaches to any individual or regulatory body.

ENFORCEMENT

Iranian courts generally enforce violations through statutorily defined remedies of the applicable law or regulation.

For example, the Cyber Crime Act provides that anyone who, by use of computer or telecommunication means, publicizes or makes accessible another individuals film, pictures or sounds, or personal or family secrets without consent, and causes loss or damage to the individual or violates that person's dignity will be sentenced to imprisonment between 61 days and six months or fined RIs 1,000,000 to 10,000,000.

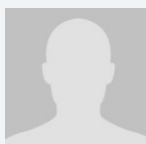
ELECTRONIC MARKETING

There is no specific electronic marketing law in Iran. However, under the Charter of Citizen's Rights, operators must obtain addressee consent before sending any advertisement. Personal cell phones are considered as a private zone. Sending any unwanted advertisements, or spam, is against the law.

ONLINE PRIVACY

There is no specific online privacy law in Iran.

KEY CONTACTS



Dr. Hassan Sedigh

CEO

Sedigh & Associates Petroleum Consultants

T +98 21 22009042 - 3

sedigh@sa-petroleum.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.