A SNAPSHOT OF DIFC DATA PROTECTION LAW (DPL) 2020

DATA PRIVACY IN UAE

JULY 2020

BDO

A SNAPSHOT OF DIFC DATA PROTECTION LAW (DPL) 2020

The new DIFC - Data Protection Law, which came into force from 1 July 2020, prescribes rules and regulations regarding the collection, handling, disclosure and use of personal data in the DIFC, the rights of individuals to whom the personal data relates and the power of the Commissioner of Data Protection in performing their duties in respect of matters related to the processing of personal data as well as the administration and application of the Data Protection Law. This Law repeals and replaces the Data Protection Law, being Law No. 1 of 2007. The Data Protection Law embodies international best practice standards and is consistent with EU regulations and OECD guidelines and is designed to balance the legitimate needs of businesses and organizations to process personal information while upholding an individual's right to privacy.

The data protection legislation is intended to protect the processing of Personal Data by a Controller or Processor or any Third Party related thereto. It also reinforces ethical data management through accountability requirements. It creates a legal and procedural framework which ensures that an individual's Personal Data in the DIFC is treated fairly, lawfully and securely when it is stored, used or released.

While the Data Protection Law is effective from 1 July 2020, businesses to which it applies will have a grace period of three months, until 1 October 2020, to prepare and to comply with it, after which it becomes enforceable.

KEY POINTS OF DIFC DATA PROTECTION LAW (DPL) 2020:

Applicability: The DPL 2020 applies in the jurisdiction of the DIFC, to the processing of Personal Data: (a) by automated means; and (b) other than by automated means where the Personal Data forms part of a Filing System or is intended to form part of a Filing System. It applies to the processing of Personal Data by a Controller or Processor incorporated in the DIFC, regardless of whether the processing takes place in the DIFC or not.

Data Protection Officer (DPO): A data protection officer should be appointed either by Controller (including a Joint Controller), or Processor, or commissioner, to independently oversee relevant data protection operations. A DPO must reside in the UAE, unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis. This is excluded for courts acting in their judicial capacity.

Data Protection Impact Assessments (DPIA): Prior to undertaking High Risk Processing Activities a Controller shall carry out an assessment of the impact of the proposed processing operations on the protection of Personal Data, considering the risks to the rights of the Data Subjects concerned.

Consent: Consent must be freely given by a clear affirmative act that shows an unambiguous indication of consent. The DPL 2020 incorporates updated strict data subject rights upon receiving and processing of the data based on the consents.

Penalty: The DPL 2020 includes the penalties for non-compliance with DPL starting from USD 10,000 to USD 100,000. These penalties includes non-compliance with various areas such as general requirements, lawful processing, obtaining consents, accountability, breach notifications, etc.

KEY POINTS OF DIFC DATA PROTECTION LAW (DPL) 2020

Breach notifications: Data controller should notify to the commissioner without undue delay, if personal data breach compromised a Data Subject's confidentiality, security or privacy. Further, Data controller should notify to the affected data subject without undue delay, if a personal data breach can result in a high risk to the security or rights of a Data Subject.

Cross-border transfer: This law describes the requirements to be taken into the consideration while transferring data out of the DIFC: (a) with adequate level of protection, (b) in the absence of an adequate level of protection; along with data sharing requirements.

Data Protection Officer (DPO) Controller Assessments: The DPO shall undertake an assessment of the Controller's Processing activities, at least once per year ("the Annual Assessment"), which shall be submitted to the Commissioner - as per the format, required contents and before the deadline.

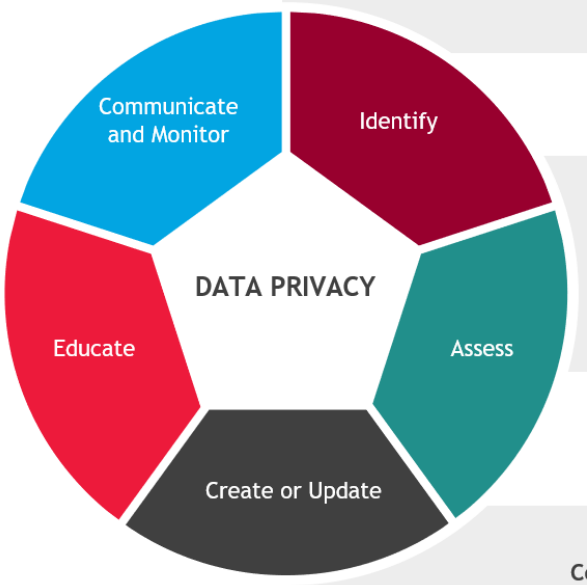
Accountability of controllers and processors: A Controller or Processor should develop and establish data protection policy and procedure which should include compliance with the DPL 2020 and resources of the Controller or the Processor, the categories of Personal Data being Processed and the risks to the Data Subjects.

AN APPROACH FOR ADOPTING DATA PRIVACY AND PROTECTION

Data breaches are not region dependent - data knows no boundaries. Data breaches and hacks lead to adverse media attention, business disruption, customer trust erosion, goodwill and reputation loss, criminal and civil penalties and costs, complaints and lawsuits and loss of revenues. Therefore, organisations should take additional measures to invest in data protection strategies by defining their policies and determining the necessary controls to protect various types of data.

Complying with the international and local regulatory standards and guidelines not only helps the organisations in preventing themselves from regulatory fines, but also helps them in maintaining the organization's reputation in the industry.

Below is an approach for adopting data Privacy and Protection in any organisation:



Identify	▶ Management commitment and support ▶ Identify and review regulatory requirements ▶ Identify stakeholders and governance mechanisms
Assess	▶ Understand and document organisation's data landscape ▶ Conduct gap assessment
Create or Update	▶ Create or update organisation's data privacy policies, procedures, privacy statements, disclaimers and other related documents ▶ Create or update data privacy controls ▶ Establish vendor risk management ▶ Establish customer request and response process ▶ Establish data privacy incident response management
Educate	▶ Provide regular trainings to all stakeholders pertaining to data privacy and protection ▶ Educate all stakeholders on how to notify in case of data breach
Communicate and Monitor	▶ Communicate data privacy related policies, notifications and disclaimers through all relevant channels ▶ Regular monitoring of data privacy related activities ▶ Notify data breach incidents appropriately to management and regulators (if any)

UNDERSTANDING DATA PRIVACY IN UAE

In the past decade, many organizations have realized the power of data, and the positive change it can bring to the organizations. It has become the most valuable asset for many organizations across the world. Data can either be business related data, or Personally Identifiable Information (PII), or Protected Health Information (PHI) or any other structured/unstructured data.

Data Privacy mostly relates to "Personal Data" of an individual, such as, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data. The Personal Data can be defined as *"Personal Data are any information which are related to an identified or identifiable natural person."*

The UAE has set in place many legislations to protect the data and the privacy of the persons and the organisations. Following are some of the UAE specific Data Privacy laws and standards with key details:

LAWS / STANDARDS	KEY DETAILS
Data Protection Law DIFC Law No. 5 of 2020	▶ The Data Protection Law prescribes rules and regulations regarding the collection, handling, disclosure and use of personal data in the DIFC, the rights of individuals to whom the personal data relates and the power of the Commissioner of Data Protection in performing their duties in respect of matters related to the processing of personal data as well as the administration and application of the Data Protection Law. The purpose of this law is to: ▶ provide standards and controls for the Processing and free movement of Personal Data by a Controller or Processor; and ▶ protect the fundamental rights of Data Subjects (the identified or Identifiable Natural Person to whom Personal Data relates), including how such rights apply to the protection of Personal Data in emerging technologies.
Privacy Protection in the UAE Penal Code	▶ Article 378 of the UAE Penal Code makes one liable if he violates the private or familial life of individuals, by perpetrating one of the following acts, unless authorised by law, or without the victim's consent: ▶ If he lends his ears, records or transmits, through a device of any kind, conversations that took place in a private place or through the telephone or any other device; and ▶ Captures or transmits, through any kind of device, the picture of a person in a private place.
Abu Dhabi - Healthcare Information and Cyber Security Standard (ADHICS)	▶ ADHICS ensures healthcare information are suitably protected to uphold public trust and reliability on governmental interest and values, and to sustain entity reputation in the provisioning of healthcare services.

UNDERSTANDING DATA PRIVACY IN UAE

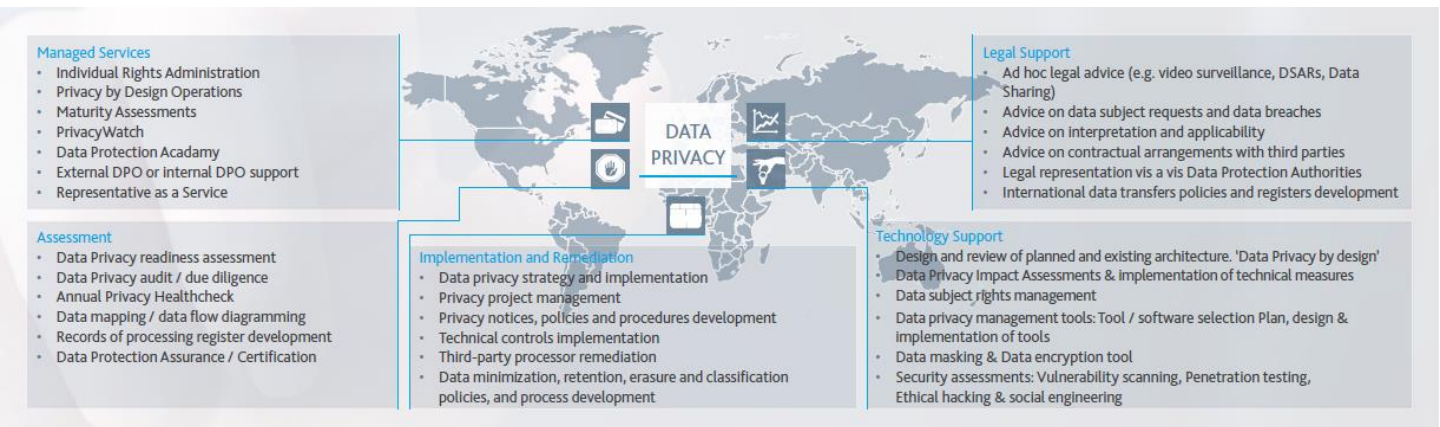
LAWS / STANDARDS	KEY DETAILS
Federal Law No. 2 of 2019 on the Use of Information and Communications Technology in Healthcare ('ICT Health Law')	UAE Federal Law No. 2 of 2019 concerning the use of information and communication technology in the area of health (the Law). The key features of this law includes: ▶ Establishment of a central IT system in healthcare sector throughout the UAE; ▶ Creation of "data protection" obligations and restrictions; ▶ Data localization: health information and data related to the health services provided in the State may not be stored, processed, generated or transferred outside the State; and ▶ With a fine of not less than AED (500,000) five hundred thousand and not more than AED (700,000) seven hundred thousand.
Federal Law No. 5 of 2012 on Combatting Cybercrimes and its amendment by the Federal Law No. 12 of 2016	▶ Federal Law No. 5 of 2012 on Combatting Cybercrimes makes it illegal to disclose any information obtained by electronic means, if such information was obtained in an unauthorised manner. ▶ Article 21 of the law makes one liable if he uses an electronic information system or any information technology means for offending another person or for attacking or invading his privacy. ▶ Article 22 of the same law makes one liable if uses without authorisation, any computer network, website or information technology means to disclose confidential information which he has obtained in the course of or because of his work.
Federal Law No. 1 of 2006 on Electronic Commerce and Transactions	▶ Federal Law No. 1 of 2006 on Electronic Commerce and Transactions provides security measures of electronic transactions and ensures that electronic data is authentic and reliable.
Dubai Data Law	▶ A Dubai Data Law is issued by the Dubai Government that governs the classification and use of Dubai data within the Emirate of Dubai. ▶ Data Providers must, in the course of data dissemination and exchange, take all the procedures required for the protection of the confidentiality and privacy of legally protected customer data. ▶ Strike a balance between data dissemination and exchange and data confidentiality and privacy.
The UAE's Constitution	▶ Article 31 of the UAE's Constitution provides for the freedom of communication by means of post, telegraph or other means of communication and guarantees their confidentiality in accordance with the law.

HOW BDO CAN HELP YOU?

BDO backed by our global and local specialists in data privacy and protection, helps organisations to understand their current data landscape, design and implement comprehensive Data Privacy and Protection strategy and roadmap to holistically improve and comply with local and Global Regulations. Following are some of our services:

- Data privacy and protection gap assessments
- Data Privacy and protection policy and procedure
- Data privacy and protection audits
- Awareness sessions and trainings
- Data Protection Officer (DPO) controller assessments
- Data privacy and protection strategy and implementation
- Data privacy vendor due diligence
- Data privacy incident management
- Data privacy maturity assessments
- Advise on Data Subject requests and data breaches
- Security operations center (SOC) for monitoring data breaches
- Vulnerability scanning, Penetration testing, Ethical hacking and social engineering

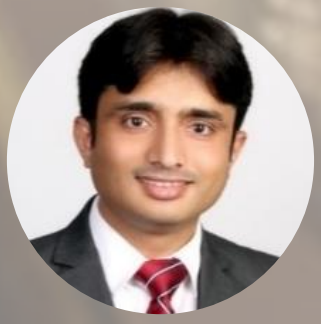
OUR GLOBAL SERVICE OFFERINGS - DATA PRIVACY



SOURCES:

- https://www.difc.ae/business/operating/data-protection/
- https://u.ae/en/about-the-uae/digital-uae/data/data-and-privacy-protection-in-the-uae
- https://www.smartdubai.ae/data/regulations
- https://elaws.moj.gov.ae/engLEGI.aspx
- https://www.difc.ae/newsroom/news/mohammed-bin-rashid-enacts-new-difc-data-protection-law/#:~:text=In%20light%20of%20the%20current,after%20which%20it%20becomes%20enforceable.

CONTACTS



Shivendra Jha
Head of Advisory

t: +971 4 518 6666
m: +971 55 572 0269
e: shivendra.jha@bdo.ae

Amit Tenglikar
Technology Advisory Services

t: +971 4 518 6666
m: +971 55 224 6250
e: amit.tenglikar@bdo.ae

For more information on BDO Data Privacy Services, please follow us on

www.bdo.ae