Introduction of the
Data Protection Law 2020 in DIFC

With rising concerns over the free movement of Personal Data and the minimal rights in place to protect the movement of data, a number of countries have come up with their own data protection laws.

In the UAE, the Dubai International Financial Center (DIFC) has issued a new data protection law called 'Data Protection Law 2020'.

The Law has come into force from 1 July 2020. A grace period of three months was provided to comply with the new regulations as enforcement began on 1 October 2020.

This article discusses the main provisions of the new Law and its impact on businesses.

What is the Law all about?

- The Law is made by the Ruler.
- The processing of Personal Data in the Dubai International Financial Centre (DIFC) is governed by the Data Protection Law, DIFC Law No. 5 of 2020 and the Data Protection Regulations.

What is the purpose of the Law?

- The purpose of the Law is to provide standards and controls for the processing and free movement of Personal Data by a 'Controller' or a 'Processor'.
- To protect the fundamental rights of Data Subjects, including how such rights apply to the protection of Personal Data in emerging technologies.

What is the applicability of the Law?

- The Law applies within the jurisdiction of the DIFC.
- The Law applies to the processing of Personal Data
  - By automated means, and
  - Apart from automated means where Personal Data forms part of a Filing System or is intended to form part of a Filing System.
- The Law 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.
- This Law applies to a Controller or Processor, regardless of its place of incorporation, that processes Personal Data in the DIFC as part of a stable arrangement, other than on an occasional basis.
- This Law does not apply to the processing of Personal Data by natural persons involved in personal or household activities that have no connection to a commercial purpose.

With this basic understanding of the purpose and application of the Law, let us delve into the common terms of the Law and their meanings.

Personal Data: Any data referring to an identifiable natural person.

Sensitive Data: Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership, as well as data on health or sex life including genetic data and biometric data, where it is used for the purpose of uniquely identifying a natural person.

Data Subject: The identified or identifiable natural person to whom the Personal Data relates.

Data Controller: Any person who alone or jointly with others determines the purposes and means of the processing of Personal Data.

Joint Controller: Any Controller that jointly determines the purposes and means of processing with another Controller.

Data Processor: Any person who processes Personal Data on behalf of a Controller.

Data Sub-Processor: Any person appointed by a Data Processor who processes Personal Data on behalf of a Data Controller and Data Processor.

Notification: Data Controllers or Data Processor should register with the Commissioner by filing a notification of processing operations, which should be kept up to date through amended notifications.

The notification should be accompanied by a fee as prescribed by the DIFCA Board of Directors.

The notifications must be re-submitted on a yearly basis of the initial notification and whenever any personal data is processed in a manner which is different to the one described in the initial notification.

Records of Processing Activities: Data Controllers need to maintain a written record (which may be in electronic form) of the processing activities undertaken which should contain at least the following information:

- Name and contact details of Data Controller, Data Protection Officer (DPO) and Joint Controller (if applicable).
- Purpose of processing data, description on the categories of Data Subjects and Personal data.
- Details of recipients to whom the Personal Data will be disclosed/shared within DIFC or outside of DIFC or to the rest of the world.
- Data retention techniques for the Personal Data collected.
- Description of technical and organizational measures implemented by the Data Controller to safeguard the data.

Data Controllers' Rights and Responsibilities

- Data Controllers must process Personal Data in a manner which is fair and lawful.
- Personal Data must be processed for a specified, explicit, and legitimate purpose determined at the time of collection on the basis of lawful grounds for legitimate processing.
- Data Controllers should keep the data accurate and up to date via erasure or rectification without any undue delay.
- Data should be kept secure and protected against unauthorized or unlawful processing, accidental loss, destruction, or damage, and appropriate technical and organizational measures should be implemented.
- Data Controllers must ensure that the Data Subject is aware of:
  - The identity of the Data Controller and how to connect to them.
  - The purpose of the collection of the data.
  - Consent is to be provided by the Data Subject to process their data by the Data Controller.
  - Other parties involved by the Data Controller to whom they will share the data for processing purposes.

Data Processors' Rights and Responsibilities

- Data Processors need to have a legally binding written agreement with Data Controllers when the processing will be performed on behalf of the Data Controller.
- Like Data Controllers, Data Processors also need to implement technical and organizational measures to protect the Personal Data of Data Subjects.
- Data Processors should also maintain a written record of all the categories of processing activities which are carried out on behalf of the Data Controller.

Data Processors can engage another processor to act as a Data Sub-Processor if they have written authorization from the Data Controller.

Data Protection Officer

- Organizations would need to appoint a Data Protection Officer (DPO) if they are engaged in High-Risk Processing Activities.
- A DPO must reside in the UAE unless he is an individual employed within the organization's Group and performs a similar function for the Group on an international basis.
- Data Controllers or Processors should publish the details of the DPO in such a manner that it is readily accessible to third parties who can contact the DPO.
- A DPO must have knowledge of this Law and its requirements and shall ensure a Controller or Processor monitors compliance with this Law.
- Data Controllers or Processors should ensure that the DPO is properly involved in a timely manner, on all issues relating to the protection of Personal Data and is given sufficient resources necessary to carry out the role.
- A Data Subject may contact the DPO of a Controller or Processor regarding all issues pertaining to the processing of his Personal Data and to exercise his rights under this Law.
- The DPO should monitor a Controller's or Processor's compliance with this Law as well as any other data protection or privacy-related laws or regulations to which the organization is subject to within the DIFC.
- The DPO is also required to conduct a Controller Annual Assessment when the DPO is appointed by the Controller and the report shall be submitted to the Commissioner as per Article 19 of the Law along with any necessary Data Protection Impact Assessments (DPIAs)

Rights of Data Subjects

The crucial rights pertaining to all Data Subjects as per the Law are listed below.

1. Right to Withdraw Consent
2. Rights to Access, Rectification and Erasure of Personal Data
3. Right to Object to Processing
4. Right to Restriction of Processing
5. Right to Data Portability
6. Automated Individual Decision-making including Profiling

Cross-border Data Transfer

- Transfer of data with an adequate level of protection can occur if the recipient country provides appropriate safeguard measures to protect the data, which includes:
  - The rule of law, the general respect for individual's rights, and the ability of individuals to enforce their rights via administrative or judicial redress.
  - Access of a Public Authority to Personal Data.
  - Existence of an effective Data Protection Law.
- Transfer of data from DIFC to other countries can occur in the absence of an adequate level of protection, provided that a sufficient safeguard mechanism is in place, which also includes:
- A Legal Binding Instrument between Public Authorities.
- Binding Corporate Rules (BCR).
- A Standard Data Protection Clause as adopted by the Commissioner.

Data Breach Notifications

- If an incident has occurred that leads to a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy, the Data Controller involved should notify the Personal Data Breach to the Commissioner as early as possible.
- Data Controllers or Processors should fully co-operate with any investigation of the Commissioner in relation to a Personal Data Breach.
- The notification to be shared with the Commissioner should:
  - Include the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate amount of Personal Data records concerned.
  - Communicate the name and contact details of the DPO or other contact point where more information can be obtained.
  - Describe the likely consequences of the Personal Data Breach and the measures taken to mitigate the risk.
- When a Personal Data Breach is likely to result in a high risk to the security or rights of a Data Subject, the Controller shall communicate the Personal Data Breach to an affected Data Subject as soon as practicable in the circumstances.

Penalties

- The Data Protection Law imposes administrative fines that may be applied for contraventions of this Law.
- The details of these fines are listed under Schedule 2 of the Law which may be updated from time to time. The penalties range from USD 10,000 to USD 100,000 as per non-compliance to specific articles listed out in the Law.

Conclusion

- **Organizations processing Personal Data need to process it lawfully, fairly, and in a transparent manner in relation to Data Subject. Data processed should be specified, explicit, and for legitimate purposes as determined at the time of collection of Personal Data.**
- **A Privacy Policy must be implemented which should state why the organization is collecting the information, how they store the information, where the information will be transferred, how they protect the information, and how the Data Subject can access their rights to gain information on their data.**
- **Organizations incorporated within DIFC or operating within DIFC need to note that Data Protection compliance is not a one-time compliance. It is a continuous journey to follow Data Protection regulations and maintain compliances on an ongoing basis to avoid any penalties or legal actions.**
- **Organizations must also know the existing and upcoming Data Protection compliances across countries as data movement occurs on a global level and data protection regulations differ in one way or another as per the law of the land.**

About Nexdigm (SKP)

Nexdigm (SKP) is a multidisciplinary group that helps global organizations meet the needs of a dynamic business environment. Our focus on problem-solving, supported by our multifunctional expertise enables us to provide customized solutions for our clients.

Our cross-functional teams serve a wide range of industries, with a specific focus on healthcare, food processing, and banking and financial services. Over the last decade, we have built and leveraged capabilities across key global markets to provide transnational support to numerous clients.

We provide an array of solutions encompassing Consulting, Business Services, and Professional Services. Our solutions help businesses navigate challenges across all stages of their life-cycle. Through our direct operations in USA, India, and UAE, we serve a diverse range of clients, spanning multinationals, listed companies, privately owned companies, and family-owned businesses from over 50 countries.

Our team provides you with solutions for tomorrow; we help you *Think Next*.

@nexdigm

*@nexdigm_*

@NexdigmThinkNext

@Nexdigm

Subscribe to our Insights

USA Canada India UAE Japan Hong Kong

Reach out to us ***ThinkNext@nexdigm.com***

www.nexdigm.com
www.skpgroup.com