CHALLENGES IN IMPLEMENTATION OF PERSONAL DATA PROTECTION LAW NO. 45 OF 2021: A CASE STUDY OF THE UNITED ARAB EMIRATES

Written by ***Irfan Ali Thanvi***

1st Year Ph.D. Student, Ahmad Ibrahim Kulliyah of Laws, IIUM, Malaysia

ABSTRACT

The Personal Data Protection Law *(PDPL)* of the United Arab Emirates is the first comprehensive federal legislation aimed at protecting the privacy of data subjects and their related rights. The UAE PDPL was promulgated on the occasion of the UAE's Golden Jubilee celebrations on 2nd December 2021, and formally enacted on 2nd January 2022 and since then has caught the attention of all the organizations and entities processing personal data. Thereby, making it crucial to understand the law and its essential obligations to understand its applicability to businesses. This whitepaper aims at analyzing the bill and drawing a comparison with other prominent legal frameworks on data privacy and protection such as the General Data Protection Regulation (GDPR)

***Keywords*:** Personal Data Protection, Cyber Law, Civil Law, UAE Laws, International Law

INTRODUCTION

For decades, the UAE government has been developing data protection laws with the objective of improving its data protection standards With the UAE government recognizing the supremacy of personal data protection and privacy, it comes as no surprise that the country has passed a federal personal data protection law The Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data ("PDPL") deals with the acquisition and processing of personal data. In the world's top 190 economies, UAE ranks 16 in ease of doing business, which makes it imperative for businesses to understand and comply with the law.[i]

THE PROBLEM STATEMENT

Previously, the legal regime in the UAE on data protection and privacy was quite fragmented since it was populated by sector-specific legislation. With the PDPL becoming enforceable in January 2022, UAE has its first enforceable federal law.[ii] It is true that the PDPL has the potential to resolve the issues inherent in the fragmented and bare minimum legislative framework in the UAE, but the introduction of this Act could result in organizations and entities processing personal data being required to comply with new provisions. Articles 249, 273, 287 and article 893 of the UAE Civil Code explain the enactments which may apply a Force Majeure to a contract, based upon circumstantial.[iii]

THE SCOPE AND APPLICABILITY OF THE PDPL

The UAE has been adaptive to the co-existence of mixed jurisdictions, the concept is equally derived from the Shariah and the French Civil Law.[iv] Articles 249, 273, 287 and article 893 of the UAE Civil Code explain the implementation of such situations which may apply a Force Majeure to the contract, when comes to implementation. These Articles give the right clue to practical situations such as construction projects, employment regulations and medical contracts. The Jurisdiction of the UAE law establishes a contractual or wrongful infringement of a legal right, as a liability on a 3D scale. The act itself, the destruction and the causal effect are the three fundamental dimensions of this nucleus, which forms the rationale of liable obligations. Albeit an intervened act is affirmed to the service provider is proven to have caused the damage rampaged through the existence of a third party, the service provider is absolved

of any liability whatsoever in this regard. Article 273(2) stipulates that in cases where the force majeure event furnishes a part of the obligation, which is impossible to perform, only that part of the contract will be terminated while the other part will be effective as per the agreement. Furthermore, Article 273(2) permits the Service Provider, in respect of the change in scenario to perform his complete obligation, to terminate the entire contract by providing notice to the recipient. If a contract is terminated or suspended under the jurisdiction of either clauses of Article 273, the subscribers of the contract will revert to square one position; if through arbitration or circumstantial developments, this becomes difficult or in some cases impossible, the courts will apply compensation to the party which suffered the loss. In a typical scenario, demurrage payment by shipment in charges in trade or maritime businesses, damages awarded to an investor by a Developer in Real Estate or in Medical liability cases, a hospital is asked to compensate a patient through the implementation of these clauses.

Although, we will be polite to a fault to evade the legal problems enfaced during such a situation, as Article 249 stipulates:

> "*If exceptional circumstances of a public nature which could not have been foreseen occur as a result of which the performance of the contractual obligation, even if not impossible, becomes oppressive for the obligor so as to threaten him with grave loss, it shall be permissible for the judge, in accordance with the circumstances and after weighing up the interests of each party, to reduce the oppressive obligation to a reasonable level if justice so requires, and any agreement to the contrary shall be void.*"[v]

The United Arab Emirates Cabinet office 2021 announced UAE's first federal data privacy law, the Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data(hereafter, PDPL). The PDPL focuses on data privacy and the rights of UAE citizens regarding sharing of their data. Thus, it applies to the processing of data involving data subjects who reside or have a place of business within the UAE and to those residing or working outside the UAE if their data is processed by a controller or processor located in the UAE. Additionally, like its western counterpart the GDPR, the PDPL also has extraterritorial application as it

applies to controllers or processors who though located outside the UAE, processes the personal data of data subjects located within the UAE.[vi]

EXEMPTIONS UNDER THE LAW

Article 3 of the PDPL, grants the Office the power to exempt those establishments that do not process a large amount of personal data from being subjected to either all or some of the requirements and conditions of the provisions of the PDPL. Presently, the activities which have been exempted from the application of this law are as follows:

"Without prejudice to any other competencies stablished for the Office under any other legislation, the Office may exempt those Establishments that do not process a large amount of Personal Data from all or some of the requirements and conditions of the provisions of Personal Data Protection stipulated herein, in accordance with the standards and controls set by the Executive Regulations of this Decree Law."[vii]

DEFINITIONS UNDER PDPL

In applying the provisions of this Decree Law, the following words and expressions shall have the meanings assigned to each, unless the context otherwise requires:

State: United Arab Emirates.

Office: The UAE Data Office established by virtue of Federal Decree-Law No. 44/2021 referred to above. Data: An organized or unorganized set of data, facts, concepts, instructions, views, or measurements, in the form of numbers, letters, words, symbols, images, videos, signs, sounds, maps, or any other form, that is interpreted, exchanged, or processed by humans or computers, which also includes information wherever it appears herein.[viii]

Personal Data: Any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking data, using identifiers such as name, voice, picture, identification number, online identifier, geographic location, or one or more special features

that express the physical, psychological, economic, cultural, or social identity of such person. It also includes Sensitive Personal Data and Biometric Data.[ix]

Sensitive Personal Data: Any data that directly or indirectly reveals a natural person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data, or any data related to the health of such person, such as his/her physical, psychological, mental, genetic, or sexual condition, including information related to health care services provided thereto that reveals his/her health status.

Biometric Data: Personal Data resulting from Processing, using a specific technique, relating to the physical, physiological, or behavioral characteristics of a Data Subject, which allows or confirms the unique identification of the Data Subject, such as facial images or dactyloscopy data.

Data Subject: The natural person who is the subject of the Personal Data.

Establishment: Any company or sole proprietorship established inside or outside the State, including companies which the federal or local government partially or wholly owns or has a shareholding therein.

Controller: An establishment or natural person who has Personal Data and who, given the nature of his/her activity, specifies the method, criteria and purpose of Processing such Personal Data, whether individually or jointly with other persons or establishments.

Processor: An establishment or natural person who processes Personal Data on behalf of the Controller, as directed and instructed by the Controller.

Data Protection Officer: Any natural or legal person appointed by the Controller or Processor to undertake the responsibilities of ascertaining the compliance of his/her entity with the controls, conditions, procedures and rules for Processing and protecting Personal Data stipulated herein and ascertaining the integrity of its systems and procedures in order to ensure compliance with the provisions hereof.

Processing: Any operation or set of operations which is performed on Personal Data using any electronic means, including Processing and other means. This process includes collection,

storage, recording, organization, adaptation, alteration, circulation, modification, retrieval, exchange, sharing, use, or classification or disclosure of Personal Data by transmission, dissemination or distribution, or otherwise making it available, or aligning, combining, restricting, blocking, erasing or destroying Personal Data or creating models therefor.

Automated Processing: Processing that is carried out using an electronic program or system that is automatically operated, either completely independently without any human intervention, or partially independently with limited human supervision and intervention.

Personal Data Security: A set of technical and organizational measures, procedures and operations, specified according to the provisions hereof, aimed at protecting the privacy, secrecy, safety, unity, integrity and availability of Personal Data.

Pseudonymization: The Processing of Personal Data in such a way that the data, after completion of Processing, can no longer be linked and attributed to the Data Subject without the use of additional information, as long as such additional information is kept separately and safely and subject to the technical and organizational measures and procedures, specified according to the provisions hereof, to ensure non-attribution of Personal Data to an identified or identifiable natural person.

Anonymization: The Processing of Personal Data in such a way that anonymizes the Data Subject's identity so that such data can no longer be linked and attributed to the Data Subject and the Data Subject can no longer be identified in any way whatsoever.

Data Breach: A breach of information security and Personal Data by illegal or unauthorized access, including copying, sending, distributing, exchanging, transmitting, circulating, or Processing data in a way that leads to disclosure thereof to third parties, or damage or alteration thereof during the processes of storage, transmission and Processing.

Profiling: A form of Automated Processing consisting of the use of Personal Data to evaluate certain personal aspects relating to a Data Subject, including to analyze or predict aspects concerning his/her performance, economic situation, health, personal preferences, interests, behavior, location, movements, or reliability.

Cross-Border Processing: Dissemination, use, display, transmission, receipt, retrieval, sharing or Processing of Personal Data outside the territory of the State.

Consent

Consent is mandatory for processing personal data. Conditions of valid consent are as follows:

(a) Consent can be given in writing or electronic form.

(b) It must be clear, simple, unambiguous, and easily accessible.

(c) The consent must indicate that the Data Subject can withdraw it at any time and must be easy to withdraw. Additionally, the withdrawal of consent must not impact the legality and law.

Conditions for Valid Consent

To protect public interest; to initiate or defend legal claims; for the purposes of occupational or preventive medicine, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services; to protect public health; for research, archival, and historical purposes; to safeguard the data subject's interests; for parties to fulfil their obligation & exercise their legal rights related to employment, social security etc.; to fulfil the contractual obligations of the data subject or to conclude, amend, or terminate contracts at the data subject's request; to comply with other State laws that impose obligations on controllers; or when processing is done on publicly available personal data via an act of the data subject or; any other cases specified by this law.

KEY REQUIREMENTS & PROVISIONS

There are several prerequisites for operations of the law:

Data Processing

The currently issued version of the PDPL is silent on data processing records, however, additional information regarding the subject may be included in the Executive Regulations.Article 22 of the PDPL prohibits the transfer of personal data to country or territory

outside the UAE unless that country ensures an 'adequate level of protection' for the rights and freedoms of data subjects in relation to the processing of personal data. Where this is not the case, Article 23 of the PDPL provides various exemptions/derogations through which personal data can lawfully be transferred across borders, including:

- creating adequate protection through appropriate safeguards (for example by using Standard Contractual Clauses ('SCCs')); and
- the data subject has explicitly consented (and the transfer does not conflict with the public and security interests of the UAE).

Further information relating to cross border transfers, including potentially a list of jurisdictions deemed as providing an 'adequate level of protection', is expected to be included in the Executive Regulations once issued.

Data Protection Impact Assessment

Under Article 21 of the PDPL, where a type of processing using new technologies that is likely to result in a high risk to the privacy and confidentiality of the personal data of a data subject, the controller is required to conduct a Data Protection Impact Assessment ('DPIA') prior to the processing.

In particular, the PDPL notes in Article 21(2) of the PDPL that the obligation to conduct a DPIA applies in the following circumstances:

- if conducting automated processing of personal information that relies on profiling and highly impacts data subjects; or
- if the processing is conducted on a large scale and includes sensitive personal data.

Where required, the DPIA shall contain, amongst other things an assessment of:

- a clear explanation of the nature of the processing activity concerned and the purpose(s) thereof;
- an assessment of the necessity of the processing in relation to its purpose;

- an assessment of the potential risks on the protection of personal information of data subjects; and
- the suggested measures to mitigate the potential risks of such processing activities.

Furthermore, controllers must review the outcomes of DPIAs regularly to ensure that processing activities are conducted in accordance with the assessment in the event that the level of risk changes (Article 21(5) of the PDPL).

Data Breach

In the case of a data breach that would prejudice the privacy, confidentiality and security of the personal data of a data subject, Article 9 of the PDPL requires that, the controller, immediately upon becoming aware of such breach, notify the Data Office of such data breach. The required notification must include details such as:

- the nature, category, reasons, approximate number and records of the data breach
- a description of the likely consequences of the data breach; and
- a description of the measures and remedial action taken by the controller to address the data breach

Cross Border Data transfers

The PDPL has extra-territorial effect and applies to:

- every data controller or data processor in the UAE who processes personal data of data subjects inside or outside the UAE; and
- every data controller or data processor established outside the UAE carrying out processing activities in relation to data subjects located within the UAE.

Material scope

The PDPL applies to the processing of personal data. 'Processing' is defined broadly as any operation or set of operations which are performed on personal data including the collection, storage, recording, organization, adaptation, modification, circulation, alternation, retrieval, exchanging, sharing, use, characterization, disclosure by transmission, dissemination,

distribution, or otherwise making available, alignment or combination, restriction, withholding, erasure, destruction, or creating models of personal data.

CHALLENGES FOR ORGANIZATIONS

The Data Protection Law promulgated on the 2nd of January 2022, although it also anticipates further executive regulations that will clarify various aspects (including the scope and level of sanctions). Controllers and processors will then have a period of six months from the date of issuance of such regulations to adjust their status and comply with the Data Protection Law.

All businesses operating in the UAE, or that are based outside the UAE, but process personal data of data subjects located in the UAE, will need to assess their activities and make changes to align with the Data Protection Law as quickly as possible. We have previously issued tips for enterprises on how to create an effective privacy framework and worked with many organisations to help them implement the required processes and policies for compliance.

HOW CAN RESIDENTS COMPLY WITH THE VARIOUS RULES & REGULATIONS?

Depending on which sector and location a business operates in, further consideration of specific sector laws and regulations, and emirate laws and regulations, may be necessary. The list of examples below is not exhaustive.

Health

Federal Decree-Law No. 2/2019 Concerning the Use of Information and Communication Technology in Health Fields including Cabinet Resolution No. 32/2020 and exceptions pursuant to Ministerial Resolution No. 51/2021 (together Health Data Law) covers the collection, processing and circulation of health data. The Health Data Law sets out data

processing, data security and data retention requirements, and places certain restrictions on the transfer of health data.

The emirates have their own health data laws. These include the Dubai Healthcare City Health Data Protection Regulation No. 7/2013 (DHCC Regulation), which applies to any 'licensee' that conducts business within the DHCC. A 'licensee' is defined in the DHCC Regulation as any licensed healthcare professional, licensed complementary and alternative medicine professional, a licensed healthcare operator, approved education operator, approved research operator, licensed commercial company, or a non-clinical operating permit holder operator.

The DHCC Regulation places restrictions on the licensee's management of patient health data, regardless of where that data might be held, and sets out the requirements for patient health data retention and transfer of patient health data.

Financial services

In the UAE financial services sector, there are a number of regulations that govern the protection of personal data. These include the Consumer Protection Regulation (Central Bank Circular No. 8/2020) and related Consumer Protection Standards, which include detailed data protection provisions. Other relevant regulations include the Central Bank Circular No. 112/2018 on Finance Companies Regulation, and Central Bank Circular No. 14/2021 Outsourcing Regulation and Standards covering banks' outsourcing activities.

Telecoms

In the UAE telecoms sector, the Telecommunications and Digital Government Regulatory Authority, the independent regulator regulating the information, communications, and telecommunications sector, has issued various regulations that include data protection provisions. These include the Internet of Things (IoT) Regulatory Policy, which applies broadly to IoT service providers and IoT service users and sets out, among other things, data classification requirements and related restrictions on cross-border data transfers.

Government data

There are also UAE government laws and regulations at the federal and emirate level covering the use of government data by government entities and government service providers. These

include the UAE Information Security Regulations and the Dubai Data Law. UAE government entities focused on the protection and use of government data include Digital Dubai, the Dubai Electronic Security Centre, and the Abu Dhabi Digital Authority.

WHAT ARE THE KEY CONSIDERATIONS FOR APPLICATION OF THESE SERVICES?

There are other federal UAE laws that cover data protection and privacy more generally. These include:

- The UAE Constitution of 1971;
- Federal Law No. 15/2020 on Consumer Protection (Consumer Protection Law) – consumers have the right to the privacy and security of their data and restrictions on its use for promotional and marketing purposes;
- Federal Decree-Law No. 31/2021 on the Issuance of the Crimes and Penalties Law (Penal Code) – the Penal Code protects against the release of "secrets", including secrets of the state. The Penal Code also refers to the protection of privacy in the case of family life;
- Federal Decree-Law No. 34/2021 Concerning the Fight Against Rumours and Cybercrime (Cybercrimes Law) – the Cybercrimes Law covers, amongst other things, the unauthorised access of personal data using IT systems.

CONCLUSION

The Law is a welcome change which will significantly impact the way companies do business in the region, increase confidence for global companies looking to do business here, and support several large-scale digital transformation projects in both the public and private sectors. We also expect that many of our clients doing business across the GCC will need to look closely at the different data protection frameworks of each jurisdiction, which are rapidly evolving and

may require specific considerations of how they differ, especially in respect of data transfers across borders. Reassuringly, the PDPL does not contain any major divergences from other well-known data protection regimes, including the GDPR. In this regard, we expect it will be welcomed by local, regional and international businesses, in particular, those that rely heavily upon personal data and international personal data flows.

BIBLIOGRAPHY

Ahmed Al-Suwaidi. (1994). Finance of International Trade in the Gulf *Volume 9 of Arab and Islamic laws series Arab and Islamic laws series: Graham & Trotman Finance of International Trade in the Gulf*. Leiden: BRILL Publishers.

Arfah Hamzah (Wan.), Ramy Bulan. (2003). *An Introduction to the Malaysian Legal System*, Kuala Lumpur: Oxford Fajar Sdn. Bhd.

Abu Dhabi Global Markets Court. https://www.adgm.com/doing-business/adgm-courts/adgm-legal-framework/adgm-courts-legal-framework/ (accessed 16 April, 2018).

B. Hunter, (2016). *The Statesman's Year Book: 1992-93*. Berlin: Springer.

Cleveland, William L & Martin Bunton. (2009). *A History of the Modern Middle East: 4th Edition.* Colorado: Westview Press.

Curtis J. Berger. (1983). *Land ownership and use*. Los Angeles: Little, Brown

Chiara Formichi. (2013). *Religious Pluralism, State and Society in Asia Routledge Religion in Contemporary Asia Series*. New York: Routledge Publishers.

Caroline Sawyer, Miriam Spero. (2015). *Succession, Wills and Probate*. New York: Routledge.

"Dubai Court System", e-services, https://www.dc.gov.ae/PublicServices/MainFlow.CMSPage. (accessed 16 April, 2018).

IBP Incorporated, (2013). *United Arab Emirates Country Study Guide Volume 1 Strategic Information and Developments*. Dakota Dunes: Int'l Business Publications.

IBP Incorporated, (2014). *UAE Insolvency (Bankruptcy) Laws and Regulations Handbook - Strategic Information and Basic Laws*, Washington DC: Int'l Business Publications.

Ibrahim Abed, Peter Hellyer, (2001). *United Arab Emirates: A New Perspective.* Cape Town: Trident Press Limited.

Martin Goodman, (2008). *Rome and Jerusalem: The Clash of Ancient Civilizations.* New York: Knopf Doubleday Publishing Group.

Muḥammad ibn Rāshid Āl Maktūm. (2013). *Flashes of Thought: Inspired by a Dialogue at the Government Summit 2013*. Dubai: Motivate Publishing Limited.

Melodena Stephens. (2017). *UAE: Public Policy Perspectives Actions and Insights - Middle East North Africa*. Bingley: Emerald Group Publishing.

Martin Lau, (2006). *The Role of Islam in the Legal System of Pakistan Volume 9 of The London-Leiden series on law, administration and development*. LEIDEN: BRILL Publishers.

Michael Grose, (2016). *Construction Law in the United Arab Emirates and the Gulf*. New York City: John Wiley & Sons.

Nathan J. Brown. (2002). *Constitutions in a Nonconstituitonal World.* New York: State University of New York Press.

Rand McNally and Company. (1905). *Rand McNally and Company.* (Chicago: Rand McNally & Company, 1905.

Roman Tomasic. (2016). *Insolvency Law in East Asia*, New York: Routledge.

Sharon Ling, *Federal Court Rules Jurisdiction to Hear Apostasy Cases Lies with Syariah Court*, STAR ONLINE (Feb. 27, 2018).

Wan Zulkifli Wan Hassan, Jamsari Alias, Nazri Muslim, Nasruddin Yunos and Azizi Umar. *The Practice of Interfaith Inheritance Distribution in Malaysia: An Analysis of its Fatwa. Middle-East Journal of Scientific Research* 22 (3): 464-469, 2014. Retrieved 18th April 2009.

ENDNOTES

[i] Doshi, Rush, Judith G. Kelley, and Beth A. Simmons. "The power of ranking: The ease of doing business indicator and global regulatory behavior." *International Organization* 73, no. 3 (2019): 611-643.
[ii] Greenleaf, Graham. "Now 157 Countries: Twelve Data Privacy Laws in 2021/22." (2022).
[iii] Donald Charrett, The International Application of FIDIC Contracts: A Practical Guide. Taylor & Francis: London, 2019, 39
[iv] Nurmohamed, Rehanna. "Shari'a Law and Its Impact on the Development of Muslim and Non-Muslim Business Relations in the United Arab Emirates: " Law and Development Review, vol. 13, no. 2, 2020, pp. 443-472. https://doi.org/10.1515/ldr-2020-0052
[v] Michael Grose, (2016). *Construction Law in the United Arab Emirates and the Gulf*. New York City: John Wiley & Sons, 81.
[vi] El-Khoury, Moufid. "The Impact of Data Protection Laws: Global and MENA Perspectives." In *2021 22nd International Arab Conference on Information Technology (ACIT)*, pp. 1-6. IEEE, 2021.
[vii] Jadalhaq, Iyad Mohammad, and Mohammed El Hadi El Maknouzi. "Reading UAE Contract Law through the Lens of Islamic Jurisprudence: A Case Study on the 'Extraneous Cause'Exception in the UAE Civil Code." *Global Jurist* 19, no. 2 (2019): 20180045.
[viii] Casoria, Maria, and Eman Mahmood AlSarraf. "The Impact of the GDPR on Extra-EU Legal Systems: The Case of the Kingdom of Bahrain." In *Personal Data Protection and Legal Developments in the European Union*, pp. 224-237. IGI Global, 2020.
[ix] Albahar, Marwan, and Mohammed Thanoon. "Privacy Regulations in the Middle East: Challenges & Solutions." (2022).