WHITEPAPER

UAE PERSONAL DATA PROTECTION LAW ('PDPL')

Insights into the new federal legislation

Overview

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 came into effect on 2nd January, 2022 and since then has caught the attention of all the organisations 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").

Target Audience

This whitepaper seeks to analyse the law and compare it to other notable legislative frameworks on data privacy and protection, like the General Data Protection Regulation. It attempts to provide an overview of the proposed law.

It will be tailored to a wide range of audiences, including senior and mid-level IT management, programme managers, and compliance leaders to help them comprehend the goals of the UAE PDPL and the obstacles they may encounter in showing compliance with this proposed legislation.

It also intends to generate discussion among secondary audiences, such as students and academics, to help them comprehend the complexities of the proposed bill.

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.

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. 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.

Structure

This whitepaper would be covering the following aspects:

- Scope & Applicability of the UAE PDPL
- Exemptions & Definitions
- Key Requirements in the PDPL
- Data Subject Rights
- Data Protection Officer
- Cross-Border Transfer
- Enforcement & Grievance Redressal
- Comparison of UAE PDPL with GDPR
- Challenges for Organizations

SCOPE & APPLICABILITY

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 UAE PDPL came into effect on January 2, 2022.

The Federal Law was accompanied by Executive Regulations , issued within six months of the law being promulgated.

The organisations were granted an additional six months from the date of issuance of execution regulation to ensure compliance with the law.

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 also 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 extra-territorial 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.

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:

Personal data held by security and judicial authorities.

Government agencies that process data.

Personal health data where there is separate legislation covering such personal data.

Subjects whose Personal Data is only processed for their own purposes.

In free zones in the UAE, companies and institutions dealing with personal information are covered by separate laws.

DEFINITIONS UNDER PDPL

1 | CONTROLLER

An establishment or natural person who possesses Personal Data and 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.

2 | PROCESSOR

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

3 | 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.

4 | SENSITIVE PERSONAL DATA

Any data that directly or indirectly reveal 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 a person.

5 | BIOMETRIC DATA

Personal Data resulting from processing, using a specific technique, relating to the physical, physiological or behavioural characteristics of a Data Subject, which allows or confirms the unique identification of the Data Subject, such as facial images or dactyloscopic data.

KEY REQUIREMENTS & PROVISIONS

1 CONSENT

CONDITIONS FOR VALID 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.

EXEMPTIONS

- 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

2 DATA PROCESSING

CONTROLS GOVERNING DATA PROCESSING

- Lawfulness, Transparency & Fairness
- A procedure for erasing or correcting inaccurate Personal Data must be in place
- Data must be collected only for a specific and clear purpose.
- Processing of Personal Data must be protected from a breach, infringement, or illegal or unauthorized processing.
- Processed personal data should be sufficient for the purpose for which they are collected and limited to that specific purposes
- The retention of personal data is prohibited following the fulfilment of the purpose for which it was processed, and can only be retained if the data controller uses the anonymization feature.
- An individual's personal data must be accurate, updated, and complete at all times.
- Any other control which may be set by Executive Regulations.

3 RECORD OF PROCESSING ACTIVITIES

For entities processing the personal data of individuals, Article 7(4) of the PDPL requires the maintenance of a special record of personal data which must be provided to the Office by the Controller when requested.

KEY ELEMENTS

- Description of categories of personal data possessed
- Details of controller and data protection officer
- Duration of the processing
- Details of persons granted authorised access, the purpose of processing, cross-border transfers, technical and organisational measures etc.

KEY REQUIREMENTS & PROVISIONS

4 SECURITY MEASURES

Under the PDPL, both the controller and the processor are required to implement measures to secure the personal data of data subjects. Following are the technical and organizational measures that have to be set in place by the controller and processor.

FOR THE CONTROLLER

- Establish appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure the confidentiality and privacy of personal data and safeguard it
- Apply measures like pseudonymization both while defining as well as during the processing of data.
- Apply the measures in respect of default settings as well to ensure that the processing is limited to the intended purpose.
- Maintain proper Records of Processing Activities
- Appoint a Processor who can implement technical and organizational measures with appropriate guarantees.

FOR THE PROCESSOR

- Protect and secure processing operations.
- Protect and secure the media and electronic devices used in the processing
- Erase or hand over the data to controller post expiry of the processing period.
- Establish appropriate technical and organizational measures and procedures to safeguard personal data when defining and undertaking the processing of Personal Data.
- Processing should be limited to purpose and set period
- Refrain from taking actions that could result in the disclosure of personal data or processing of the same.
- If more than one processor is involved, set in place a contract defining their processing-related obligations, responsibilities and roles.

KEY REQUIREMENTS & PROVISIONS

4 SECURITY MEASURES

COMMON CONTROLS

- Measures like encryption and pseudonymization.
- Measures to ensure the safety, validity, confidentiality and flexibility of processing.
- Measures to ensure timely retrieval and access of personal data in case of a physical or technical failure.
- Measures to ensure smooth testing, evaluation and assessment of the effectiveness of technical and organizational.
- Measures to evaluate and assess the effectiveness of technical and organizational measures.

5 DATA PROTECTION IMPACT ASSESSMENT

Under the PDPL, both the controller and the processor are required to implement measures to secure the personal data of data subjects. Following are the technical and organizational measures that have to be set in place by the controller and processor. Processing is likely to pose a risk to privacy and confidentiality if data Subjects are assessed comprehensively based on automated Processing, including Profiling, which may have legal consequences or may seriously affect them or a large amount of Sensitive Personal Data will be processed.

KEY ELEMENTS OF A DPIA

- A clear description of what the processing activity is and its purpose(s);
- Analyzing the necessity of the processing in light of its meaning;
- Risk assessment of the protection of personal information of data subjects

KEY REQUIREMENTS & PROVISIONS

6 DATA BREACH

Article 1 of the PDPL, defines a data breach as illegal or unauthorised access to information security or personal data, which includes copying, sending, distributing, exchanging, transmitting, circulating or processing data in a way that leads to the disclosure thereof to a third party, or that damages or alters the data during storage, transmission, or processing.

ELEMENTS

- The controller upon becoming aware of a data breach incident is obligated to inform the Data Office of the same.
- The notification to the Data Office must include the following information:
- The nature, category, reasons, approximate number and records of the data breach.
- An explanation of what may result from the data breach.
- Data breach measures and remedial action was taken by the controller.

7 CROSS BORDER DATA TRANSFERS

Similar to the GDPR, the cross-border transfer provisions under the PDPL can be classified based on the existence of an adequate level of protection.

- An adequate level of protection is said to be available if there is special legislation on personal data protection or if there is a bilateral or multilateral agreement between the UAE and the recipient country.
- In the absence of an adequate level of protection, data can be transferred if a contract or agreement is laying down obligations related to data protection, the transfer is based on the express consent of the data subject, the transfer is necessary to fulfil legal obligations and establish exercise or defend legal rights or for the execution of a contract or international judicial cooperation or the protection of the public interest.

DATA SUBJECT RIGHTS

The Right to Stop Processing

The Data Subject can request the controller restrict or stop the processing in the following cases:

1. If the accuracy of Personal Data, is being objected then the Processing shall be restricted to a specific period to allow verification of the same by the Controller.
2. If the Processing violates the agreed purposes.
3. If the Processing violates the provisions hereof, and the legislation in force.

1.

The Right to Obtain Information

Based on a request submitted to the Controller, the data subject is entitled to obtain the following information for free

1. The types of his/her personal data that are processed.
2. Purposes of processing.
3. Decisions are made based on Automated Processing, including Profiling.
4. Targeted sectors or establishments with which his/her Personal Data is to be shared, whether inside or outside the State.

2.

The Right to Object to Automated Processing

Any decision involving Automated Processing, including profiling, that has legal consequences or seriously affects the Data Subject has the right to be objected to by the data subject.

However, it is not applicable:

1. If the automated processing is included in the terms of a contract
2. It is necessary by-laws
3. If the data subject has already given his/her consent to that automated processing.

3.

The Right to Request Personal Data Transfer

The Data Subject has the right to obtain his/her Personal Data provided to the Controller in a structured and machine-readable manner if such processing is based on consent or is necessary for the fulfilment of a contractual obligation and is made by automated means.

The Data Subject has the right to request the transfer of his/her data to another Controller whenever this is technically feasible.

4.

DATA SUBJECT RIGHTS

The Right to Correction

If the Data Subject's inaccurate personal data is held with the controller, he or she has the right to request the controller to correct or complete the information without undue delay.

5.

The Right to Restrict Processing

A Data Subject may object to and stop the processing of his/her Data in the following circumstances:

1. If the Processing is for direct marketing purposes, including profiling related to direct marketing.
2. If the Processing is to conduct statistical surveys unless the Processing is necessary to achieve the public interest.
3. If the Processing violates the provisions of Article (5) hereof.

6.

Communication with Controller

Data Subjects must be provided with appropriate and clear ways and mechanisms to establish communication with the controller regarding their rights and related requests.

7.

The Right to Erasure

cData Subject also has the right to request the erasure of his/her Personal Data if:

1. If it is no longer required for the purposes for which it is collected or processed.
2. If the consent is withdrawn by the Data Subject.
3. If the data subject objects to the processing or if there are no legitimate reasons to continue processing.

8.

DATA PROTECTION OFFICER

A DPO must be mandatorily designated if thE processing undertaken includes:

- Systematic and extensive evaluation of sensitive data
- Profiling and automated processing
- Utilises modern technologies likely to cause high risk to the personal data
- A large scale of sensitive data

A DPO can be an existing employee, or another individual appointed by the organization, from within or outside of the UAE.

RESPONSIBILITIES OF A DPO

- Ensure legal and regulatory compliance by the controller or the processor.
- Ensure the existence and effectiveness of the measures implemented.
- Provide appropriate advice regarding existing measures, conduct periodic assessments, and document the results of these assessments.
- Respect the confidentiality of personal information when performing their duties under the provisions of the PDPL and the Executive.
- Receive data subject requests and act as a point of contact.

RESPONSIBLITIES OF CONTROLLER AND PROCESSOR

- Inclusion of the DPO at an appropriate time in matters relating to the protection of personal data.
- Assist with the necessary support and resources.
- Ensure that the position of the DPO does not result in a conflict of interest with their existing role.
- No penalty should be imposed on the DPO for performing their duties according to the law.

ENFORCEMENT & GRIEVANCE REDRESSAL

The UAE PDPL outlines the rights of the data subjects with respect to the enforcement of the provisions and subsequent imposition of penalties in case of non-compliance by the organisations.

Article 24 of the PDPL

- Article 24 of the PDPL provides a data subject with the right to file a complaint with the Data Office.
- This can be on the grounds of violating PDPL provisions by the controller or processor while undertaking the processing of personal data.

Article 25 of the PDPL

- Article 25 also grants the data subjects the right to submit a written grievance against any decision, administrative penalty or procedure taken against him/her by the Office.
- A grievance must be sent to the Office General Manager in a written format within thirty days from the date of receiving the notification of such an administrative penalty.

Article 26 of the PDPL

- Presently, the PDPL does not define any penalties for breaches.
- However, upon receiving a complaint from a data subject to the UAE Data Office, the Council of Ministers can impose administrative fines.

COMPARISON WITH GDPR

SI . No.	Basis of Comparison	PDPL / GDPR
1.	Scope / Applicability	• The PDPL is broader than the GDPR in the aspect that it automatically applies to the processing of data of UAE residents by non-UAE organisations unlike, the GDPR whose application in such scenarios is conditional. • The PDPL however like the GDPR does not apply to processes undertaken by a non-EU organisation in the context of activities carried out by an EU-based organisation. • The PDPL also has a specific application to the data subjects who have a business or reside in the UAE.
2.	Data Subject Rights	The rights vested with data subjects under the are: 1. Right to access 2. Right to request the transfer 3. Right to be forgotten 4. Right to restrict 5. Right to object 6. Right to object to automated processing However, there are exceptions, unlike GDPR where the data controller can reject a data subject's request if the information is not covered under the PDPL or if the request is overly repetitive etc.
3.	Processing of children's data	Unlike the GDPR, the PDPL does not lay down any specific provisions for the processing of children's data.

COMPARISON WITH GDPR

Sl. No.	Basis of Comparison	PDPL / GDPR
4.	Legal Basis for Processing	Under the GDPR, there are 6 lawful bases for the processing of data however, under the PDPL the primary basis is consent unless an exception applies
5.	Obligations of Controllers/ Businesses/ Covered Entities	Like GDPR, the PDPL contain a general security obligation for controllers and processors.
6.	Data Protection Officer	While both PDPL and GDPR lay down the requirement of appointing a DPO, situations demanding mandatory appointments are different. • Under the PDPL, a DPO is to be appointed when the processing would cause a high risk to the privacy of the data subject as a consequence of adopting new technologies, the processing would involve a systematic and comprehensive assessment of sensitive personal data, including profiling and automated processing, and/or where the processing will be made on large volumes of sensitive personal data. • Additionally, it also provides details of the resources to be provided to a DPO to be able to carry out their responsibilities efficiently.

COMPARISON WITH GDPR

Sl. No.	Basis of Comparison	PDPL / GDPR
7.	Consent	Similar to the GDPR, consent under the PDPL too needs to be a specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data by a statement or by clear affirmative action, whether in writing or electronically. Other consent requirements laid down by both legislations are similar.
8.	Penalties	Presently, the PDPL does not define any penalties for breaches. However, upon receiving a complaint from a data subject to the UAE Data Office, the Council of Ministers can impose administrative fines
9.	ROPA	Bothe PDPL and GDPR require the maintenance of records of processing activities. The PDPL lays down some additional information to be included such as the details of the person authorised to access personal data
10.	Data Protection Impact Assessment	• Under the GDPR, high risk is measured with reference to the impact of processing on the rights and freedoms of a natural person whereas under the PDPL, the risk is measured corresponding to the impact on privacy and confidentiality of personal data. • Further, DPIA requirements under the PDPL are limited to the use of "modern technologies" whereas under the GDPR the requirement to carry out a DPIA is not limited to the use of new technologies

COMPARISON WITH GDPR

Sl. No.	Basis of Comparison	PDPL / GDPR
11.	Transparency	There is no express requirement in the PDPL for the controllers to share private information with the data subjects.
12.	Data Breach	Both the GDPR and PDPL obligate the processor to inform the controller of any breach incident. However, under the PDPL, the obligation to notify the data office applies to all breaches unlike the GDPR wherein such notification is not mandatory if the breach is unlikely to result in a risk to data subjects.
13.	Exception	The GDPR allows the data office to exempt organisations that do not undertake the processing of large volumes of data, however, such a provision is not available under the GDPR
14.	International Transfers	• Both legislations follow the adequacy rule. • Under the PDPL, the cross-borer transfer of data is possible in exceptional situations in the absence of fulfilment of the adequacy requirement. apply. For example, the data subject has provided explicit consent and the transfer is not in conflict with the public or security interests of the UAE, or if the transfer is necessary to perform obligations or to execute a contract with the data subject.
15.	Marketing	• Under the PDPL, personal data can be used for direct marketing as long as the same is consented to by the data subject. • Under the GDPR the processing of personal data for direct marketing is based on the grounds of legitimate interest. Both the GDPR and PDPL grant their data subjects the right to object to the processing of personal data for direct marketing.

CHALLENGES FOR ORGANIZATIONS

1. The PDPL is required to operate alongside existing laws in the UAE's financial-free zones. It will co-exist with the Data Protection Law Dubai International Financial Centre Law No. 5 of 2020 and Abu Dhabi Global Market's Data Protection Regulations 2021.

2. Additionally, specific legislations for the protection of banking and credit data as well as health information are also to be complied with. The existence of multiple laws has led to the creation of a complex and fragmented privacy landscape which is difficult for organisations to navigate and comply with.

3. The law also grants the data protection authority the power to exempt establishments that do not process a large amount of data. However, there is no clarity regarding what constitutes a "large" amount of data thereby, making it difficult for organisations to understand whether or not they fall under the said exemption.

4. The primary ground for processing under the PDPL is granting of consent by the data subject. This can make it difficult for organisations to process personal data according to the law as the majority of them rely upon legitimate interest as a catch-all category.

5. Further, the UAE law provides for several exceptions such as the processing of data by government agencies and these many carve-outs might make it difficult to establish bilateral reciprocity which will then impact an organisation's ability to process personal data.

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

- https://www.dataguidance.com/notes/uae-data-protection-overview
- https://b9n6x6m2.rocketcdn.me/wp-content/uploads/2022/01/2021-UAE-Personal-Data-Protection-Law-Japanese-Translation-AMERELLER.pdf
- https://www.lexology.com/library/detail.aspx?g=15a5e38d-4453-46d4-99e7-49ccd9d1cab6
- https://smex.org/uaes-data-protection-law-between-exceptions-and-exemptions/
- https://www.twobirds.com/en/insights/2021/uae/how-does-the-new-uae-federal-decree-law-on-personal-data-protection-compare-against-the-gdpr#:~:text=Legal%20basis%20for%20processing,individual%20unless%20an%20exception%20applies.

tsaaro

WHY TSAARO?

Tsaaro provides privacy and cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include Privacy compliance, DPO-as-a-service, Vulnerability Assessment & Penetration Testing, Cyber Strategy, DPIA to name a few, delivered by our expert privacy professionals recognized by IAPP.

Akarsh Singh
(CEO & Co-Founder, Tsaaro)
Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

Sasikanth Akhilesh
(Director of Privacy, Tsaaro)
Sasikanth Akhilesh is a Certified Information Privacy Manager and also a Certified Information Privacy Professional/Europe (CIPP/E). He has extensive experience in the field of data privacy and compliance.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Tsaaro Netherlands Office
Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31-686053719

Tsaaro India Office
Manyata Embassy Business Park, Ground Floor, E1 Block, Beech Building, Outer RingRoad,
Bangalore- 560045
India
P: +91-0522–3581

Email us
info@tsaaro.com