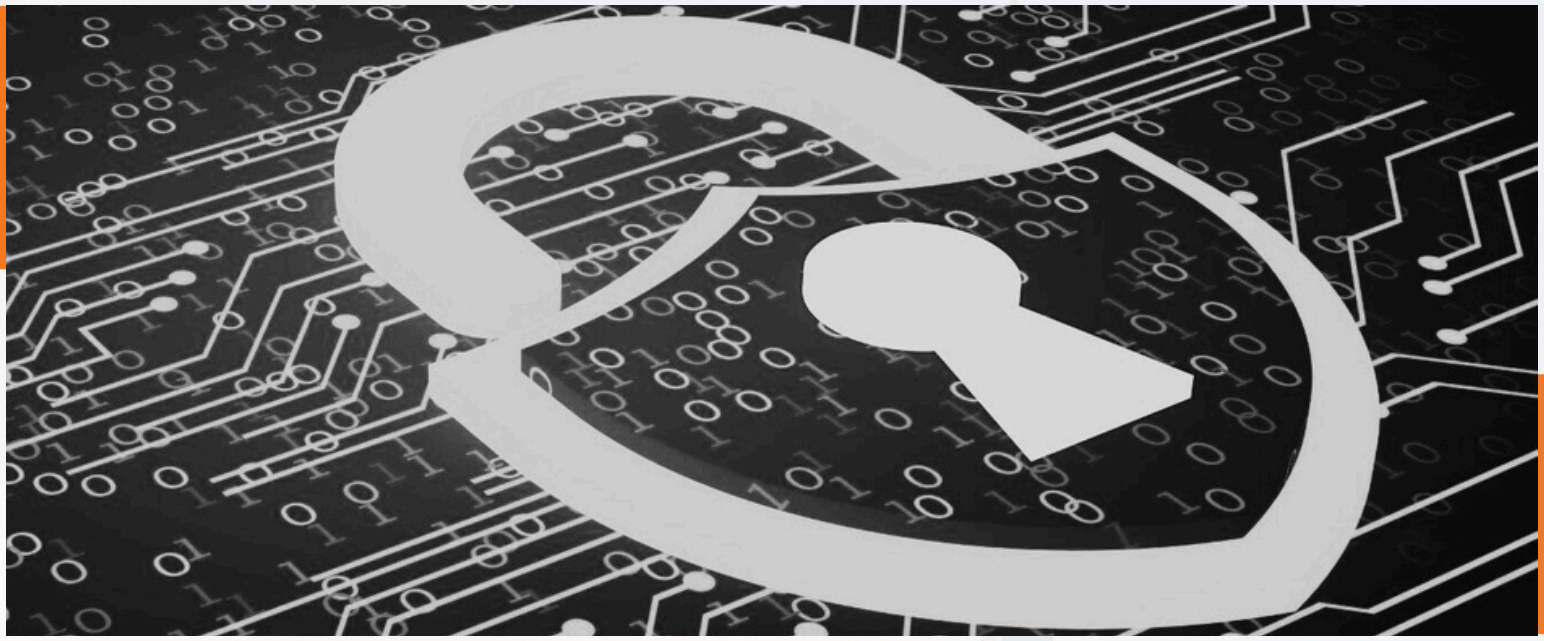
REINA CONSULTING
Tax and Legal Consultants



Data Protection Law in the UAE

With the advent of digitization, free flow of information and data has increased, which has made personal data the most critical asset which needs protection from being misused. The regulation for processing of personal data has become a primary objective of modern regulatory frameworks as businesses increasingly rely on digital systems, cloud infrastructure, and large-scale data processing. Accordingly, several countries have enacted laws and regulations for protecting the privacy rights and regulation of data flow. In response to the developments in the realm of privacy and data protection laws, the United Arab Emirates (UAE) enacted the **Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL)**, establishing the country's first comprehensive federal framework governing the processing of personal data.

The PDPL came into effect officially on 2 January 2022 introducing a structured regime regulating how entities collect, use, store, and transfer personal data as well as sensitive personal data. However, it is expected to be fully enforceable once the executive regulations are in place providing for enforcement actions by the relevant authority. The law reflects the UAE's broader objective of strengthening digital governance while aligning its regulatory framework closely with the General Data Protection Regulation.

While certain financial free zones in the UAE maintain their own privacy frameworks such as the DIFC Law No. 5 of 2020 applicable in the Dubai International Financial Centre and the Data Protection Regulations 2021 applicable in the Abu Dhabi Global Market (ADGM), the PDPL constitutes the principal legislation governing personal data processing for entities operating in the mainland UAE. Understanding the key provisions of the law is therefore essential for businesses handling personal data within the jurisdiction.

1. Scope of Applicability

The PDPL applies to the processing of personal data carried out through electronic systems or other structured means. Its scope of applicability extends not only to data subjects residing or established within the UAE, but also to establishments and natural persons located in UAE and processing personal data of data subjects located inside or outside the UAE. Further, PDPL also applies to establishments and natural persons located outside the country, mainly foreign entities, where the processing relates to personal data of data subjects located within the UAE.

At the same time, the law excludes certain categories of data or entities from its application like; (a) Government data, (b) government entities which control or process personal data, (c) data processed for personal purposes, (d) personal data held by security or judicial authorities, (e) data governed by sector-specific legislation, such as personal health data or banking and credit information and (f) companies or establishments located in UAE free zones and having special legislations regarding personal data protection.

2. Key Concepts

The PDPL establishes a set of foundational definitions that govern the entire legislative framework.

Personal data is broadly defined as any information relating to an identifiable natural person. This includes identifiers such as names, identification numbers, images, location data, or other characteristics that may be used to identify an individual. The law also recognises specific categories of **sensitive personal data**, including information revealing health status, biometric data, genetic data, religious beliefs, or criminal records, which are subject to enhanced protection.

Data subject being the natural person to whom the personal data relates.

The legislation distinguishes between the two primary stakeholders involved in the processing of personal data: (a) a **controller** is the entity that determines the purposes and means of processing personal data, while (b) a **processor** is an entity that processes personal data on behalf of the controller and under its instructions. These roles are crucial to the allocation of compliance obligations under the law.

3. Importance of "Consent" for Processing of Personal Data

The PDPL enshrines 'consent' as the primary basis for processing personal data of the data subject unless a specific exception as specified under the law applies. Consent must be clear, specific, and unambiguous, and must indicate that the data subject has authorised the processing of their personal data through a clear positive statement or action.

The law, however, recognises certain exceptions in which personal data may be processed without obtaining consent from the data subject. These exceptions include (a) processing necessary to protect public interest, (b) where personal data has been made publicly available by the data subject, (3) processing required to establish or defend legal claims, (4) for purposes of occupational or preventive medicine, (5) to protect public health, (6) for archival purposes or for scientific, historical and statistical studies, (7) for exercising legally established rights in the field of employment, social security or laws concerned with social protection, (8) for performance of a contract to which the data subject is a party or any other legal requirements.

4. Obligations of Controllers and Processors

Processing Controls

The law sets forth processing controls which must be strictly observed by entities while handling personal data. Entities are required inter alia to collect data only for specific and clearly defined purposes, process personal data in a fair, transparent and lawful manner, must ensure that subsequent processing is not incompatible with those purposes and limited to what is necessary to achieve the intended purpose of processing.

All entities are under a continuing obligation to maintain the accuracy of personal data, taking appropriate steps to rectify or erase information that is no longer correct. Once the purpose of processing has been served, retention must not extend beyond what is necessary, unless the data has been anonymised in a manner that prevents identification of the data subject concerned.

Implementation of Measures

Controllers are required to implement appropriate technical and organisational measures to ensure the security and confidentiality of personal data. These measures should be proportionate to the nature of the data being processed and the risks associated with the processing activity. Additionally, controllers must also maintain internal records describing the categories of personal data processed, the purposes of processing, the persons authorised to access the data, and the technical safeguards implemented to protect the data.

Processors, on the other hand, must process personal data strictly in accordance with the instructions of the controller and must implement appropriate safeguards to protect the data throughout the processing lifecycle.

Data Breach Notification and Governance

In the event of any breach occurring that could affect the privacy or security of personal data, the controller must notify the UAE Data Office and provide details regarding the nature of the breach, the number of individuals affected, and the corrective actions taken to mitigate the incident.

In cases where the breach may directly affect the rights or privacy of individuals, the controller must also notify the affected data subjects.

The law also requires entities to appoint a **Data Protection Officer** in specific circumstances, particularly where processing activities involve large volumes of sensitive personal data or where processing activities present a high risk to individuals' privacy.

5. Rights of Data Subjects

The PDPL grants data subjects, rights of access, correction, erasure, and restriction in relation to their personal data. The right of access covers information on data categories, processing purposes, recipients, and cross-border transfer safeguards. Erasure may be sought where data is no longer necessary or consent has been withdrawn. Data subjects may also object to certain forms of processing and challenge automated decisions that carry legal or significant effects.

6. Cross-Border Transfers of Personal Data

In principle, cross-border transfers are permitted where the receiving jurisdiction provides an adequate level of protection for personal data. Where such protection cannot be demonstrated, personal data may still be transferred under certain conditions, including where appropriate contractual safeguards are implemented or where the data subject provides explicit consent for the transfer.

The law also recognises specific circumstances in which cross-border transfers may be necessary, such as where the transfer is required to fulfil contractual obligations or to establish or defend legal claims.

Conclusion

The PDPL marks a significant milestone in the evolution of the UAE's regulatory framework offering businesses a coherent and predictable structure for managing their data processing obligations. By establishing clear principles governing the collection, consent, use, and transfer of personal data, the legislation provides businesses with a structured foundation for responsible data governance.

Far from being merely a regulatory burden, the PDPL presents a meaningful opportunity for businesses operating in the UAE. A robust data protection framework fosters consumer confidence, strengthens contractual relationships, and reduces vulnerability to data-related disputes and penalties. Businesses that embed the PDPL's principles into their operations — from consent management and data accuracy to individual rights and cross-border transfer safeguards — are better positioned to attract international partners, meet investor expectations, and sustain long-term growth in an increasingly data-driven economy.

Thus, for businesses operating in the UAE, compliance with the PDPL requires a proactive approach that integrates legal compliance, internal governance mechanisms, and robust data security practices. As digital transformation continues to reshape business operations across sectors, entities that prioritise responsible data protection will be better positioned to manage regulatory risks and maintain the trust of customers and stakeholders.

Please share your suggestions and feedback at
info@reina-consulting.com

Reina Consulting

Office No. B102, 1st Floor, Block B, Saraya Avenue Building, 65 Street, Al Garhoud,
Dubai, United Arab Emirates
www.reina-consulting.com

Dubai | Delhi (NCR)

reinaconsulting-uae
Follow our LinkedIn page for regular updates