Handbook for complying to UAE's Data Protection Law

paramount
@ssuring Value

grcp@paramountassure.com

Introduction

As the organizations in the middle east gear up for a privacy-regulated environment, the awareness about data privacy and its importance is spreading rapidly among the residents of middle east countries. This makes it challenging for organizations to protect the rights and freedom of these residents while balancing the business goals.

Privacy and Data protection is a techno-legal domain that has never seen this kind of traction earlier. The synergy needed between the organizational departments includes development and maintenance of a robust privacy framework, establishment of data subjects' rights mechanism, periodic review of privacy controls, notification of data privacy breaches to Data Protection Authorities, adherence to the legal obligation of controllers and processors and so on. Thus, achieving privacy compliance is a cross-functional responsibility and requires organization-wide effort.

Why is UAE's data protection law significant?

As the global market for data privacy started exploding couple of years ago, countries in the middle east also started revamping the data protection laws to ensure that the rights and freedom of the residents are empowered and protected.

UAE being a leader in digital space needed a future-proof data protection law that would apply to the technological advancements. Data is highly unsegregated and there is no control over how it is shared over the network. While the earlier sectoral data protection laws addressed this aspect up to some extent, a federal data privacy law was the need of the hour. With this new data protection law, UAE has established a new direction for businesses and has ensured a sense of trust in the global technology market.

This law opens various avenues to explore such as levelling with the international standard for data privacy, acting as a pioneer in the privacy space, enabling secure personal data transfer to countries outside UAE, gaining more trust in the country's legal system, and providing appropriate choice to the data subjects.

Thus, we see a multi-faceted advantage for businesses, consumers, and the country.

What are the Key requirements of the Law?

UAE's Personal Data Protection Law (PDPL) is very similar to the already established modern age data privacy laws across the globe such as GDPR, CCPA, etc. The law came into force on Jan 2, 2022, and the executive regulations are expected to be published by anytime soon. Organizations will then have 6 months to meet the requirements and demonstrate compliance. Now let's look at the key requirements of the law and understand the compliance obligations.

Who all are covered under the law?

UAE's Personal Data Protection Law protects the rights of data subjects who are domiciled in UAE or have a place of business in UAE.

Which organizations need to comply with the law?

UAE's PDPL specifically covers two types of entities or organizations:

1. Controllers/Processors inside UAE, irrespective of whether they process Personal Data of UAE residents
2. Controllers/Processors outside UAE, but process Personal Data of UAE Data Subjects

What are the key principles of the law?

- Processing must be fair, transparent, and lawful
- Processing must be done only for the purpose for which the Personal Data was collected
- The Collection of personal data must be minimized only for the purpose necessary. Data collected must be compatible with the purpose of processing
- Personal data must always be kept accurate and up to date. There must be a mechanism to erase or correct data that is collected
- Appropriate technical and organizational measures must be implemented to ensure the protection of personal data from data breaches or leaks
- Personal data must be retained only for a time during which the purpose is met. However, personal data can be retained if it is anonymized, and the data cannot be attributed to a data subject
- Personal data must be processed only as per the executive regulations

When can an organization process personal data?

Processing of personal data without the consent of the data subject is prohibited unless the processing pertains to

- Protection of public Interest
- Data that is made publicly available by the data subject
- Data that is necessary to initiate or defend in case of any judicial or security procedures
- Data that is necessary for the occupational or preventive medication of an employee and provision of health/social care under legislation in force in the State
- The data that is necessary to protect public health
- Scientific, historical, and statistical work
- Protection of rights of data subjects
- Processing is required by the controller/processor to perform its obligation in recruitment, social security, or social protection
- Performance of contract a data subject has entered in to with an organization
- Compliance with obligations set out in other laws of the State
- Any other situations put forth by executive regulation

What are the conditions for processing based on Consent?

Processing personal data based on consent is challenging. This is because of the difficulty in the implementation and tracking of consents from the data subjects. Moreover, UAE's PDPL has laid down strict conditions, as mentioned below, for organizations to opt for consent as a legal basis of processing.

Track the consents provided by the data subjects

Must be clear, unambiguous, and easily accessible in both electronic and written form

Data Subject Rights and right to withdraw consent at any time must be communicated

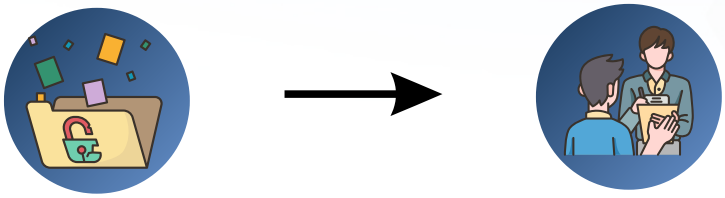
Withdrawal of consent must not affect previous processing of personal data

What roles do Controllers & Processors play? (Article 7 & 8)

- Implement technical and organizational measures to protect Personal data, including where automatic processing of personal data is identified
- Implement privacy controls to comply with Article 5 of the regulation, including but not limited to consent management, data retention and deletion, data integrity and anonymization
- Maintain a record of processing for all the processing activities involving personal data in an organization
- Perform vendor risk assessments before appointing controllers/processors and implement measures and controls to ensure that personal data is protected
- Analyze risks to the rights and freedom of data subjects arising due to the processing of PD
- Controllers and Processors shall assess and document risks associated with the processing
- The controller must conduct a Data Protection Impact Assessment prior to carrying out a processing activity which can likely risk the personal data of data subjects
- Controller and processors must appoint a Data Protection Officer who shall monitor compliance of controllers/processors with the provisions of the law and its executive regulations
- Assist The Office with the information needed upon the decision of the competent judicial authority
- The processors shall process personal data only upon written instructions from the controller

What is the breach reporting mechanism?

Breach notification is an important part of UAE's Data protection law as this directly relates to the transparency principle of data privacy. It is the responsibility of the controller to report breaches/anticipated breaches to The UAE Data Office. Requirements for notification of the breach to both The Data Office and data subjects affected are outlined in the law.



1. While notifying the breach to The UAE Data office, the following information must be supplied:

- Description, nature, form, extent, data subjects affected etc.
- Details of Data Protection Officer
- Potential effects of the breach
- Steps taken to mitigate the effect of breach
- Documentation of breach and corrective actions taken
- Any other information requested by The Office

2. The controller must notify the Data Subjects affected by the breach and the risk to the privacy, confidentiality and security of their personal data
3. It is the responsibility of the processor to notify any personal data breaches to the controller and the controller in turn must report it to The Office

What rights are provided to the data subjects?

The law empowers data subjects of the organizations with certain rights. These rights are not absolute and are bound by certain limitations. The following rights can be exercised by data subjects:

- Right of access to information
- Right to request personal data portability
- Right to rectification or erasure of personal data
- Right to restriction of processing
- Right to stop processing
- Right of processing and automated processing

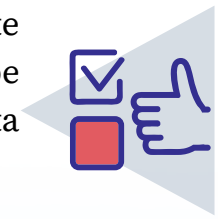
Is there any restriction for cross border data transfer?

As per the Law, cross-border data transfer is allowed under certain circumstances.

When a country is deemed to be 'Adequate' by The Office. In this case, there can be a free flow of personal data to these countries

The countries have a bilateral or multilateral agreement in respect to the protection of personal data

When a country is not deemed to be 'adequate,' appropriate measures and controls such as contracts or agreements must be signed to protect personal data. In such cases, explicit consent of data subjects must be taken for transferring personal data outside UA



Few other cases where cross border data transfer is allowed:

- The transfer is necessary for judicial purposes
- The transfer is based on the performance of a contract
- The transfer is based on the protection of public interest

Penalties associated with Non-compliance

The penalties and sanctions pertaining to the contraventions of the law and the executive regulations will be issued by the Director-General of the Office.

Complaint Lodging and grievance redressal

Data subjects have the right to lodge a complaint against a controller/processor in case he/she has reasons to substantiate that the organizations have been mishandling his/her personal data protected by the law. Concerned parties further have the right to challenge the decision given by the Office within 30 days of the notification of the decision.

Exemptions

This law does not apply to:

- government data and processing of personal data by government authorities
- the processing of Personal Data by security or judicial authorities
- data subjects who process personal data purely for personal purposes
- health data/financial data governed by special regulations/legislations
- banking or credit personal data governed by a specific legislation
- organizations governed by Special Data Protection Regulations under free state
- The Office has the authority to exempt any organization from this regulation under certain circumstances

Paramount's Approach towards UAE PDPL

Paramount Computer Systems is the regional leader of Cybersecurity in the Middle east. With the right mix of people, processes and technology we help our customers reach maturity in the security and privacy space. Our Data Privacy service offering focuses on building processes and embedding technology to enable businesses to grow while meeting the regulatory compliance requirements.

Paramount's data privacy services are aligned to meet privacy journey of an organization, be it the start of the journey or achieving maturity. The various kinds of services we offer within Data Privacy Services are:

Gap Assessments

Provide advisory and consulting services depending on the maturity of the privacy program of an organization

Advisory and Consulting

Provide advisory and consulting services depending on the maturity of the privacy program of an organization

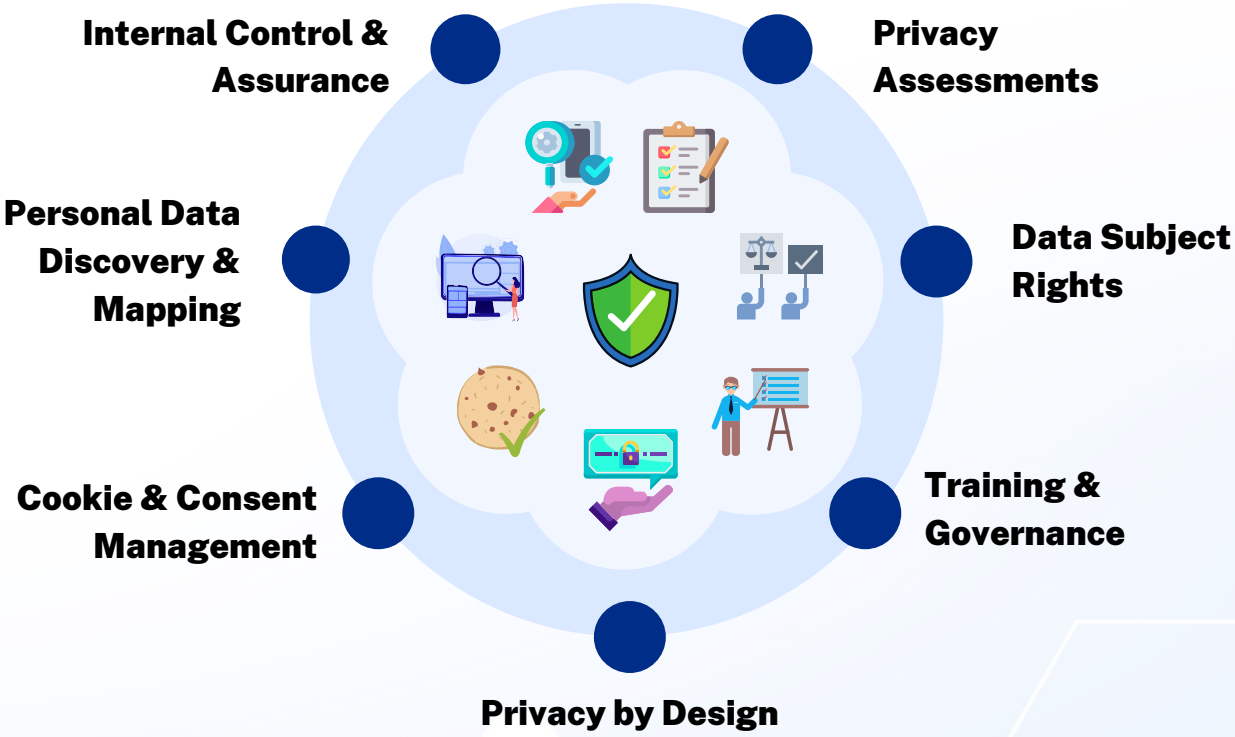
Implementation Services

Implement the data privacy program within the organization including implementation of privacy tools

Continuous Monitoring

Establish a privacy governance program, track privacy risks, provide training to the employees and automate Privacy dashboard

Data Privacy Service Portfolio



Key Differentiators

- Technology driven Privacy program implementation
- Multi-regulatory coverage across middle east
- Qualified and experienced professionals (CIPP/E, CIPM, CIPT, FIP, etc.)

Contact Us

For more information related to Data Privacy Services, kindly contact us at **grcp@paramountassure.com**

Please note that this book provides an overview and interpretation of the law.
For the official text of the law refer to the authorized sources.