Compliance Handbook for Saudi Arabia's Personal Data Protection Law (PDPL)

paramount
@ssuring Value

grcp@paramountassure.com

Contents

1. Introduction to Saudi Arabia PDPL

As countries in the Middle East develop and enact personal data protection laws across the region, it becomes essential for organizations to ramp up their systems, processes and people-skills to meet the regulatory compliance requirements. In a very similar effort, the Saudi Authority for Data and Artificial Intelligence (SDAIA) has published the first ever Personal Data Protection Law (PDPL) in the Kingdom. It is mandatory for the controllers and processors to adhere to the compliance requirements of PDPL and establish a robust Personal Data Protection Program to uphold the Data Privacy rights of the residents of the Kingdom.

This effort towards establishing PDPL is in alignment with the requirements of NDMO Domain 14 (Personal Data Protection) requirements published back in the year 2021. Organization needs to develop synergy needed between the business departments including the development and maintenance of a robust privacy framework, establishment of individuals' 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 becomes a cross-functional responsibility and requires organization-wide effort.

This handbook will act as a guiding document to understand the requirements from the law and high-level steps required to achieve Saudi PDPL compliance.

2. Significance of Saudi Arabia PDPL

Recognizing the need to establish an international regulatory and legal framework to protect individuals' and organizations' digital sovereignty and data privacy in Saudi Arabia, the Personal Data Protection Law (PDPL) was enacted.

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, Saudi Arabia 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 Saudi Arabia, gaining more trust in the country's legal system, and providing appropriate choice to the individuals. Thus, we see multi-faceted advantage for businesses, consumers and the country.

3. Timeline

The Saudi Arabia Council of Ministers has given approval to a series of changes to the PDPL. The new amendments have been implemented via Royal Decree No. M147 of 5/9/1444H dated 27 March 2023, and as a result, the PDPL will now come into effect in September 2023. The executive regulations supplementing the PDPL should be issued prior to this date. Organizations under the scope of the law must comply with its provisions by September 14, 2024.

4. Applicability of the Law

The law applies to any processing of personal data related to individuals that take place in Saudi Arabia by any means. In case of foreign entities, if the processing is related to individuals residing in Saudi Arabia, the PDPL applies.

Organizations

The PDPL covers two types of entities or organizations:

1. Controllers/Processors inside Saudi Arabia, irrespective of whether they process personal data of its residents.
2. Controllers/Processors outside Saudi Arabia, but processing personal data of its individuals.

5. Key Data Privacy Principles

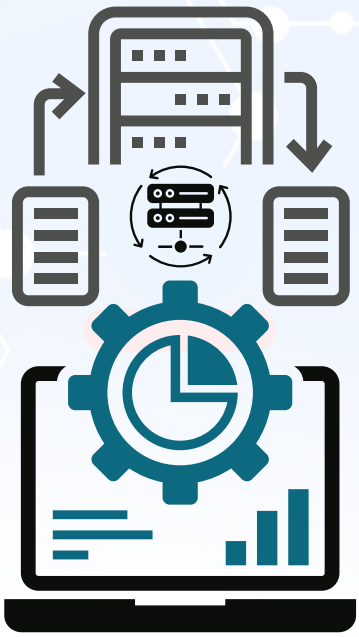
- Processing must be fair, transparent, and lawful.
- Processing must be done only for the purpose for which the Personal Data was collected.
- The Collection of personal data must be minimized only for the purpose necessary. Data collected must be compatible with the purpose of processing.
- Personal 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, following which the data shall be disposed of.

6. Compliance Requirements under the Law

6.1. Conditions for processing

- Apart from certain exceptions created under the Law, neither Personal Data may be processed nor the purpose of Processing of Personal Data may be changed without the consent of the Data Subject.
- Further conditions of the consent are proposed to be set out by the Regulations which would also provide the cases in which the consent must be express, and the terms and conditions related to obtaining the consent of the legal guardian where the Data Subject fully or partially lacks legal capacity.
- The Law also allows the Data Subject to withdraw their consent, the rules of which will also be set by the Regulations.

Processing of personal data without the consent of the individual is prohibited unless:



- The Processing serves the actual interests of the Data Subject, but communicating with the Data Subject is impossible or difficult.
- The Processing is pursuant to another law or in implementation of a previous agreement to which the Data Subject is a party.
- The Controller is a Public Entity and the Processing is required for security purposes or to fulfill judicial requirements.
- The Processing is necessary to achieve a lawful interest of the Controller or any other party, without prejudice to the rights and interests of the Data Subject and provided that the Personal Data is not Sensitive Personal Data.

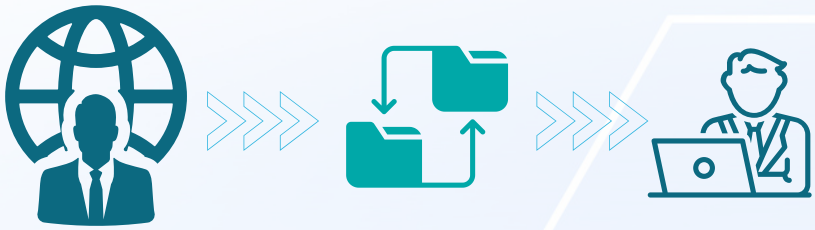
6.2. Personal data of a special nature

Sensitive Personal Data (Ethnic origin or race, religious, intellectual, or political belief, criminal and security data, biometrics, Genetic, Credit, Health Data, and data that indicates that one or both of the individual's parents are unknown) may not be processed without explicit consent of the data subject and unless it is collected directly from the Data Subject. The Regulations shall set out the rules and conditions applicable in this regard.

6.3. Roles of Controllers & Processors

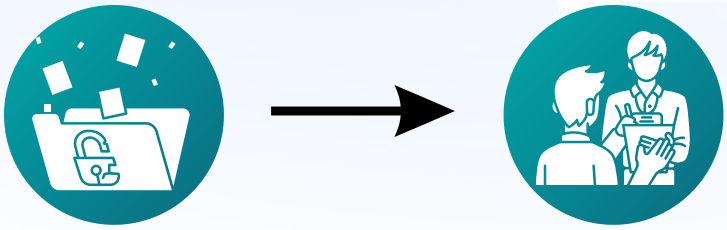
- The controller shall make a privacy policy available to the Data Subjects prior to data collection, outlining what personal data will be collected, the purpose of collection, how it will be collected, stored, processed, and destroyed, data subject rights, risks from not collecting personal data, the identity of the controller along with the contact details of its representatives; information on disclosure, and cross border transfers.
- The Controller shall destroy the personal data without undue delay when the purpose of the Collection ceases to exist except when the retention is permitted or if the data subject is de-identified in accordance with the Regulations.
- The Controller shall notify any correction or amendment of the personal data to all the other entities to which it has been transferred and make the amendment available to such entities.
- The controller shall collect personal data only for related purposes and in accordance with the legal provisions and shall specify if the purpose of collection is mandatory or optional.
- The controller may collect Personal Data only from the Data Subject unless the exceptions under Article 10 are applicable.
- The controller may not process Personal Data without taking sufficient steps to verify the Personal Data accuracy, completeness, timeliness and relevance to the purpose for which it is collected in accordance with the provisions of the Law.

- The Controller shall take all the necessary organizational, administrative and technical measures to safeguard Personal Data, including during the Transfer of Personal Data, in accordance with the provisions and rules set out in the Regulations.
- Controller shall ensure that the processor provides guarantees necessary to implement the PDPL.
- The Controller shall verify the selected Processor's compliance with the provisions of this Law and the Regulations.



6.4. Breach Notification

Breach notification is an important part of Saudi Arabia's PDPL as this directly relates to the transparency principle of data privacy. If the Controller becomes aware that the Personal Data has been leaked, damaged or illegally accessed, and such leakage, damage or access is capable of causing harm to the Data Subject or is detrimental to the rights or interests of the Data Subject, the Controller shall carry out the notification requirements relating to the leakage of Personal Data, in accordance with the rules and provisions set out in the Regulations, and the provisions set by the Competent Authority.



6.5. Data Subject Rights

The law empowers individuals of the organizations with certain rights. The following rights can be exercised by the individuals:

- Right to be informed
- Right to access
- Right to request correcting, completing or updating their Personal Data
- Right to request the Destruction of their Personal Data
- Right to obtain their Personal Data in a legible and clear format
- Right to request the Transfer of their Personal Data to another Controller

The controller may restrict the said rights if it is:

- Necessary to protect Data Subject or others from harm, or
- For security purposes, to implement another law, or to fulfill judicial requirements.

6.6. Cross-border data transfers and disclosure

Controllers are permitted to transfer Personal Data outside the Kingdom if the country to which the Personal Data is to be transferred has

Regulations that ensure appropriate protection of Personal Data and protection of the rights of Data Subjects, and

A supervisory entity that imposes appropriate procedures and measures on Controllers to protect Personal Data meeting the standards provided under this Law.

The Competent Authority shall adopt evaluation criteria for the abovementioned requirements.

The Controller may also make cross-border transfers irrespective of the above criteria under the following circumstances:

- It is for preserving the public interest, public health, public safety, or protecting the life or health of a specific individual or individuals.
- It is related to performing an obligation under an international agreement to which the Kingdom is a party.
- It is done in the performance of an obligation of the Data Subject, in accordance with the applicable provisions set out in the Regulations.

In all instances of cross-border transfers, the controller should ensure that

- Such transfer shall not adversely affect the national security or vital interests of the Kingdom.
- The Transfer or Disclosure of Personal Data shall be limited to the minimum amount of Personal Data required.

6.7. Disclosure to third parties

The Controller can only disclose Personal Data with the consent of the Data Subject, from publicly available sources, to public entities for security purposes, to protect public health/interest/life, or for lawful interests that don't infringe on the rights of the Data Subject. The Regulations provide rules and procedures for each case with exceptions to Article 16.

6.8. Penalties associated with non-compliance

Any person who discloses or publishes Sensitive Personal Data with the intention of causing damage to the Data Subject or achieving a personal benefit can be punished by imprisonment of up to **2 years** or a fine of up to **3,000,000 Saudi Riyals** or both.

The penalties and sanctions pertaining to any other contraventions of the law may attract either a warning or a fine up to **5,000,000 Saudi Riyals**.

The penalty should be proportionate to the nature and seriousness of the violation and the resulting damage. The court also has the discretion to double the fine for repeated violations provided that the fine does not exceed double the maximum limit.

6.9. Complaint lodging and grievance redressal

Data Subjects may submit any complaint to the Competent Authority or the Controller pertaining to the Law and the Regulations. The Regulations shall further set out the rules for handing the complaints.

7. Exemptions

This Law shall not apply to the Processing of Personal Data by an individual for personal or family use, as long as the Personal Data is not published or disclosed to others. The Regulations shall specify the personal and family uses referred to in this paragraph.

8. Paramount's Approach for Compliance

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

Assess existing data privacy gaps within the organization against applicable laws on the basis of a privacy control checklist and offer recommendations.

Advisory and Consulting

Assist in establishing organization wide data privacy framework, governance structure and mitigate Data Privacy risks to meet regulatory requirements.

Implementation Services

Drive data privacy processes through automation and provide support at each phase of data lifecycle.

Post-Implementation Training

Provide role-based and certification trainings for employees of the organization.

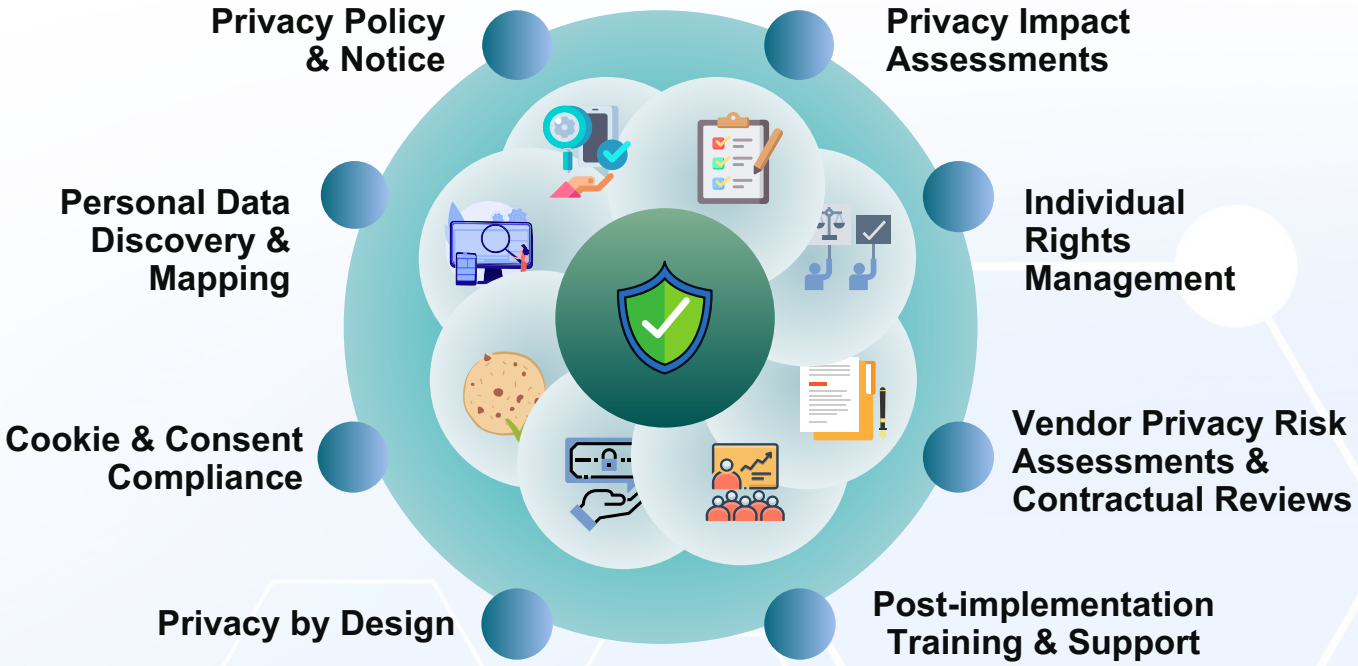
Continuous Monitoring

Monitor privacy governance program through continuous risk assessments.

Data Privacy Audits

Support in conducting internal data privacy audits followed by recommendation roadmap.

9. Paramount's Data Privacy Offerings



10. Salient Differentiator of Paramount's Services

- Technology-driven Privacy program implementation.
- Local team presence in GCC for addressing multi-regulatory requirements.
- Qualified and experienced professionals (FIP, CIPP/E, CIPM, ISO 27701).

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.