protiviti®
Global Business Consulting

Insights into KSA's Personal Data Protection Law

The Personal Data Protection Law of the Kingdom of Saudi Arabia was implemented by Royal Decree M/19 of 16 September 2021, approving Resolution No.98 dated 14 September 2021 ('PDP Law') and published in the Official Gazette on 24 September 2021. The Saudi Authority for Data and Artificial Intelligence (SDAIA) stated on 22 March 2022 announcing the decision to postpone full enforcement of the PDP Law till 17 March 2023. The PDP Law will be supported by Executive Orders, which provide detailed guidelines and standards for companies to achieve compliance with the Law.

The below article is based on the PDP Law published in 24th September 2021 and considers the draft executive regulations published in March 2022. On 20 November 2022, the Saudi Data and Artificial Intelligence Authority (SDAIA) launched a public consultation on proposed amendments to the Personal Data Protection Law. Furthermore, various provisions under the proposed amendments are subject to executive regulations which are yet to be published. Once the amendments are finalized a subsequent point of view shall be published to cover the same.

Scope of PDP Law:

PDPL is applicable to:

any processing of personal data related to individuals that takes place in the Kingdom by any means

- Organization established outside KSA but if they are processing personal data of individuals residing in KSA
- Organizations established in KSA

Exclusions

The PDP Law does not apply to an individual's processing of personal data for purposes that do not exceed personal or family use, provided the data is not published or disclosed to others by the individual.

1. The term 'Personal Data Owner' used in the PDP Law refers to an individual to whom the personal data belongs, his representative, or whoever has legal guardianship over him.
2. The PDP Law also applies to processing personal data relating to deceased individuals if such data would lead to identifying the individual or their family members.

Violation of the provisions stated in the Law may introduce the following fines and penalties

1

Disclosing or publishing sensitive data in violation of the provisions of the Law will result in imprisonment for a period not exceeding two years and/or a fine not exceeding SAR 3,000,000.

2

Infringement of the cross-border data transfer provisions stated within the Law will result in imprisonment for a period not exceeding one year and/or a fine not exceeding SAR 1,000,000.

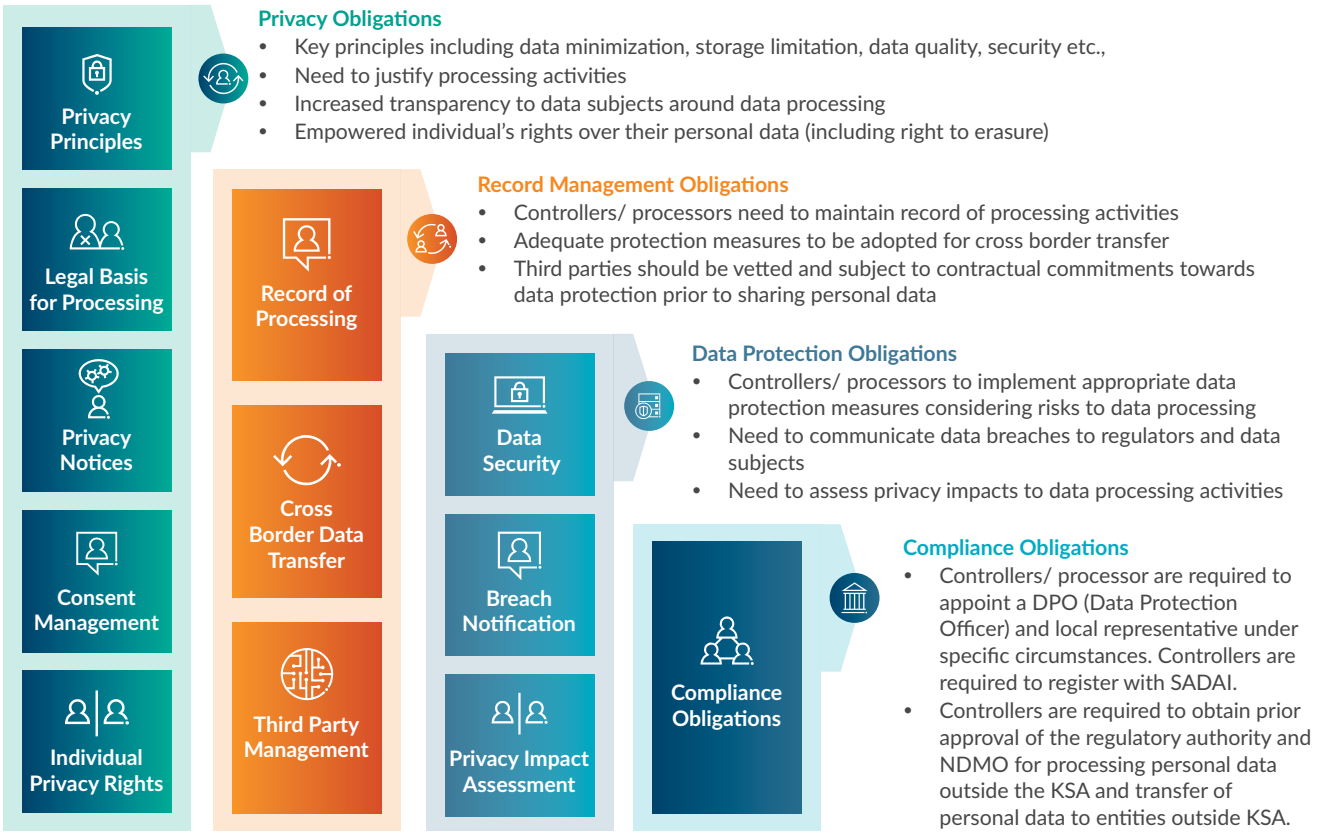
3

Violation of any other provisions of the Law or the Regulations may also result in warning or a fine not exceeding SAR 5,000,000. The penalty may be doubled in case of repeat violation, even if the fine exceeds the maximum limit subject to the fine not exceedingly double this limit.

Core Elements of the Law

The PDP Law combines the leading practices from of various current, world-class data protection laws, such as the GDPR, CCPA, and other forward-thinking, technology-agnostic concepts. The key requirements of the PDP Law cut across various areas, including risk, compliance, legal obligations, data protection, data governance, and record management. This calls for a holistic, structured, and collaborative approach to be adopted by companies to establish a privacy program that helps uphold the privacy rights of individuals and ensure compliance.

The section below provides a high-level overview of the fundamental obligations:



What Should Companies Do?

The PDP Law brings about a paradigm shift in the way companies view the collection and processing of personal data impacting businesses across Industries that are involved in the processing of personal data. The section below illustrates specific critical considerations for companies to navigate the PDP Law Compliance journey:

Visibility over Personal Data

Companies in KSA have been undergoing a massive transformation journey with technological advancements and digital transformation initiatives over the last few decades that have increased the exposure to large volumes of data including personal data. Multiples requirements in the PDP Law and draft executive orders stipulate stringent requirements concerning the processing of personal data, such as fulfilling Personal Data Owner requests, ensuring a lawful basis exists for the processing of personal data, data retention/disposal, and additional requirements concerning the protection of sensitive data, credit data, health data, and children's data. In light of these requirements companies must gain complete visibility over personal data and its processing activities, emphasizing the need to first carry out a ***data discovery*** exercise to identify and map out the collection, storage, processing, and transfer of personal data within its environment.

Ensuring Processing is Fair and Legitimate

Personal data and associated processing activities are part and parcel of the day-to-day business operations. While the PDP Law does not restrict companies from collecting or processing personal data, it does expect companies to ensure that personal data is processed in a lawful, fair, and transparent manner.

It is essential for companies to re-look at their business processes to ensure the processing of personal data is legitimate and aligned to the acceptable lawful basis identified under the PDP Law. Furthermore, companies should review and update their privacy policies/ notices to increase transparency over their processing activities concerning of collecting and using their data. Additionally, companies should establish/ update mechanisms to obtain and record consent (where necessary) from Personal Data Owners to continue processing their data unless an alternative lawful basis exists.

Upholding Individual's Privacy Rights

Under the PDP Law, Personal Data Owners have rights over their data, including the "right to be informed", "right to information and access", "right to correction/rectification" and "right to erasure". As an example, this would mean that the Personal Data Owner can request companies for a copy of all personal data or ask for correction/ deletion of specific personal data. Under the draft executive orders, companies are expected to fulfil such requests within 30 days of receiving the request which may be extended to a further duration of 30 days if the request requires extraordinary efforts. Further, under the draft executive orders, additional obligations and Personal Data Owner rights apply for processing activities involving emerging technologies like artificial intelligence.

To address these requirements, Companies need to enforce better control over personal data, establish standard operating procedures, and leverage technology solutions to manage the lifecycle of such requests received from Personal Data Owners to ensure timely fulfillment of Personal Data Owners.

Addressing Data Localization and Cross-border transfer concerns

The PDP Law prohibits the transfer of personal data outside KSA except under certain exemptions allowed under the law. Under the recent draft executive orders, personal data cannot be transferred outside KSA before conducting an impact assessment and obtaining the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a case-by-case basis. In addition, under the draft executive orders, an adequacy list (of countries) is expected. Incase transfers are required to countries not part of the adequacy list would be subject to additional requirements.

Companies that have a global presence, entities outside KSA, utilize cloud hosting, or leverage outsourcing arrangements, may need to relook at the data hosting/ transfers, carry out an impact assessment, seek approval from Regulatory Authority and Competent Authority, and adopt adequate safeguards to continue processing/ transfer of personal data outside KSA.

Use of Third Parties

Companies constantly engage third party services providers to support their business processes. The advent of the PDP Law, the traditional approach towards vendor onboarding and management should be relooked. The PDP Law requires companies to implement additional measures before sharing personal data with third-party vendors ("Data Processors"), such as conducting data privacy and security due diligence before hiring third parties, incorporating contractual obligations around data privacy and security, and regularly monitoring compliance.

Consent Management

The PDP Law recognizes 'Consent' as one of the primary lawful basis to justify processing activities which may require companies to seek and obtain the informed consent of the Personal Data Owner to start/continue the processing activities. Additionally, mechanisms to facilitate consent withdrawal should be established, which should be as seamless as the process for obtaining consent. Further, the recent draft executive orders mandate Data Controllers to obtain explicit consent from Personal Data Owners before sending marketing/advertising materials through personal means of communication. Additionally, the draft executive orders provide specific requirements concerning the processing of children's data, such as consent of any person under the age of 13 may only be obtained from the legal guardian of such person.

Companies should relook at their consent collection and management practices to ensure that consent obtained from Personal Data Owner is informed, specific, and unambiguous. Further, companies must maintain records to prove that consent was obtained and are expected to enable accessible mechanisms for consent withdrawal.

Privacy Impact Assessment

The PDP Law requires companies to assess the privacy impact of any product/ service provided to the public if it involves processing personal data. Under the draft executive orders, companies may also be required to carry out privacy impact assessments of processing activities that meet specific criteria (such as processing of sensitive data, use of emerging technologies, use of monitoring or tracking technologies, automated decision making, cross border transfers, etc.) to ensure data privacy risks are proactively identified/ mitigated to minimize impacts to Personal Data Owners. Additionally, companies may need to present the privacy impact assessment results to Senior Management to agree on risk treatment options. In some instances where the impact assessment identifies high risks that lack adequate treatment options, the Data Controller should report to the Regulatory Authority for further consultation with the Competent Authority.

These requirements expect the establishment of a robust risk management practice by companies across KSA especially those in the B2C sector to ensure their products/ services/ data processing activities undergo privacy impact assessments (ideally as part of the ideation/ design stage).

Specific obligations for Data Processors

The PDP Law recognize specific obligations for data processors that process personal data upon detailed particular instructions from data controllers. This would mean that processing activities (carried out by service providers within the region or outside), concerning Personal Data owners in the Kingdom, are regulated under the PDP Law. These obligations include, ensuring the purpose of processing is aligned with the written instructions of the Data Controller, implementing appropriate technical and organizational safeguards, and following proper data retention/ disposal procedures.

Data processors providing products/ services to companies in KSA should take note of these obligations to ensure the lawful processing of personal data as they also fall under the PDP law and executive orders.

Breach Notification

The PDP Law requires companies to immediately report data breaches or violations of personal data concerned that may impact their privacy, confidentiality, or security to the Competent Authority and in certain circumstances to Personal Data Owners as well. Further, the executive orders stipulate 72 hours as timelines for breach notification (to Competent Authority) and further elaborate the criteria when such information should be sent to Personal Data Owners.

Considering the expectations, including timelines specified in the draft executive orders, companies should relook at their security monitoring and incident management program to ensure early identification of potential data breaches. Further, the incident management processes should be integrated to effectively identify privacy incidents, and procedures should be defined to manage breach notification requirements.

Registration of Data Controller

The PDP Law requires Data Controllers of private legal capacity to register themselves in the Competent Authority's portal. Additional regulations are expected to follow regarding the procedures and conditions for registration including relevant fees.

Appointment of Data Protection Officer (DPO)

Under the PDP Law, Data Controllers will be required to designate one or more of its employees who should be charged with the responsibility to govern and oversee the implementation of the Privacy Program and compliance with this regulation. Further, companies outside KSA that fall under the applicability of this law should appoint a representative in the Kingdom licensed by the competent authority to perform his obligations stipulated under the provisions of the Law and the Regulations. Further, the executive orders call out the need for companies to appoint a Personal Data Protection Officer as needed at the discretion of the Competent Authority.

Considering the various requirements in PDP Law, Data Controllers should consider establishing a function to govern, monitor and manage the personal data protection program. It is recommended to ensure the function is established and is not impacted by conflicting responsibilities..

Data Retention and Disposal

Under the PDP Law and draft executive orders, personal data should only be retained until the purpose of its collection ceases to exist or for an additional period required:

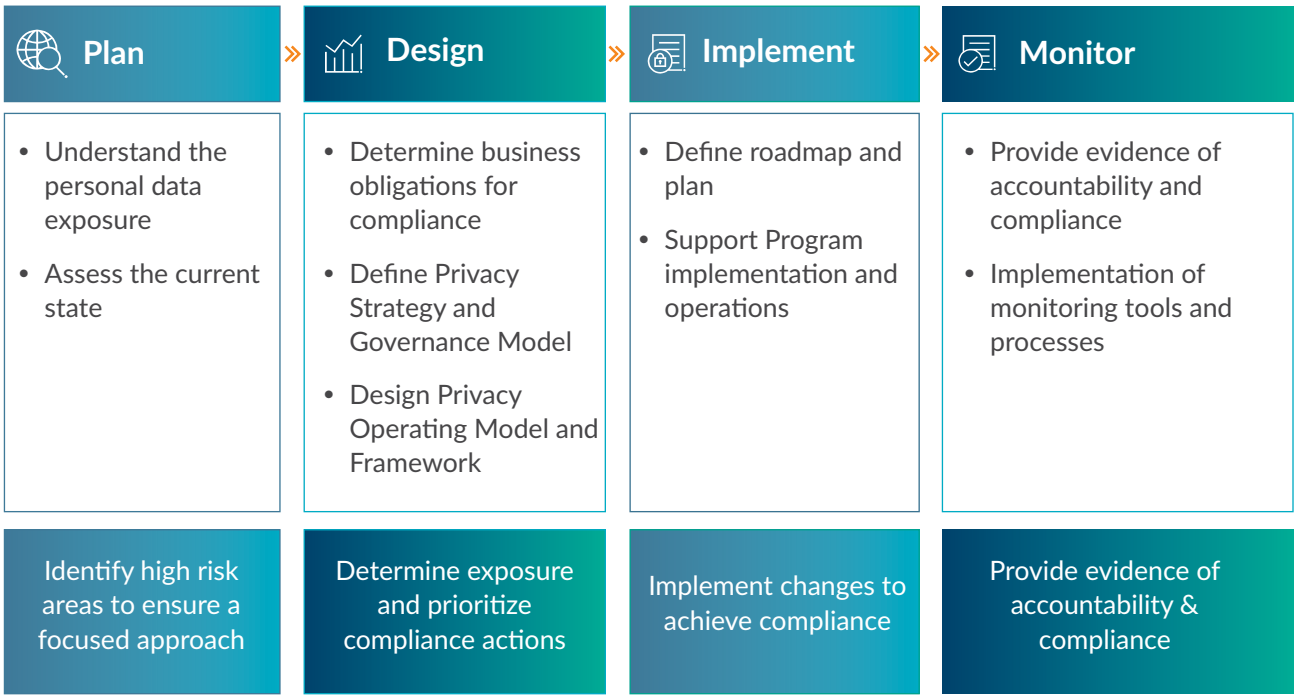
- Under other applicable Laws or,
- If it is related to a legal case pending before the judicial authority.

This requirement expect companies to establish a formalized program to identify the categories of data handled, clearly define the retention policy and schedules, and implement data disposal practices that ensure personal data is not used/ retained beyond lawful purposes.

While the above list highlight some of the key obligations for companies, it is imperative for companies to establish a formalized Data Privacy Program to govern, manage, operate, and monitor business processes and supporting technologies to ensure compliance with the PDP Law and executive orders. This would require companies to develop policies and procedures, assign roles and responsibilities, formalize a risk management program, and establish mechanisms for governance for effectively managing Data Privacy risks and ensuring compliance with the PDP Law requirements.

How Protiviti can support?

Protiviti supports clients in achieving compliance with the PDP Law requirements through a phased approach. Our approach is flexible and identified by the following four key phases to help clients with their privacy compliance obligations. Using this approach, we have supported many clients in their privacy journey.



Duration of each phase and level of effort is highly dependent on personal data processed, the size and scope of company's environment and process complexity and maturity.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Niraj Mathur
Managing Director
Email: niraj.mathur@protivitiglobal.me

Sriram Sivaramakrishnan
Managing Director
Email: sriram.s@protivitiglobal.me

Siva S
Managing Director
Email: siva.s@protivitiglobal.me

Sourabh Sharma
Managing Director
Email: sourabh.sharma@protivitiglobal.me

Our offices in Middle East Region

Abu Dhabi
Al Ghaith Holding Tower
9th Floor, Airport Road
P.O. Box: 32468, Abu Dhabi
United Arab Emirates
Phone: +971.2658.4640
Email: abudhabi@protivitiglobal.me

Bahrain
Platinum Tower, 17th Floor
Bldg. 190, Rd. 2803, Blk. 428, Seef
P.O. Box: 10231, Diplomatic Area
Manama, Kingdom of Bahrain
Phone: +973.1710.0050
Email: bahrain@protivitiglobal.me

Dubai
U-Bora Tower 2, 21st Floor
Office 2104, Business Bay
P.O. Box: 78475, Dubai
United Arab Emirates
Phone: +971.4438.0660
Email: dubai@protivitiglobal.me

Egypt
Cairo Complex
Ankara Street Bureau 1
Second Floor, Sheraton Area
Heliopolis - Cairo, Egypt
Phone: +20.22.586.4560
Email: egypt@protivitiglobal.me

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al-Waleed Street
Sharq P.O. Box: 1773
Safat 13018, State of Kuwait
Phone: +965.2242.6444
Email: kuwait@protivitiglobal.me

Oman
Al Ufuq Building, 2nd Floor
Office No. 26, Shatti Al Qurum
P.O. Box: 1130, PC 112
Ruwi, Sultanate of Oman
Phone: +968.2469.9403
Email: oman@protivitiglobal.me

Qatar
Palm Tower B, 19th Floor
P.O. Box: 13374, West Bay
Doha, Qatar
Phone: +974.4421.5300
Email: qatar@protivitiglobal.me

Saudi Arabia
Al-Ibdaa Tower, 18th Floor
Building No. 7906, King Fahad
Branch Road, Al-Olaya, P.O. Box 3825
Riyadh 12313, Kingdom of Saudi Arabia
Phone: +966.11.298.7100
Email: saudiarabia@protivitiglobal.me

protiviti®