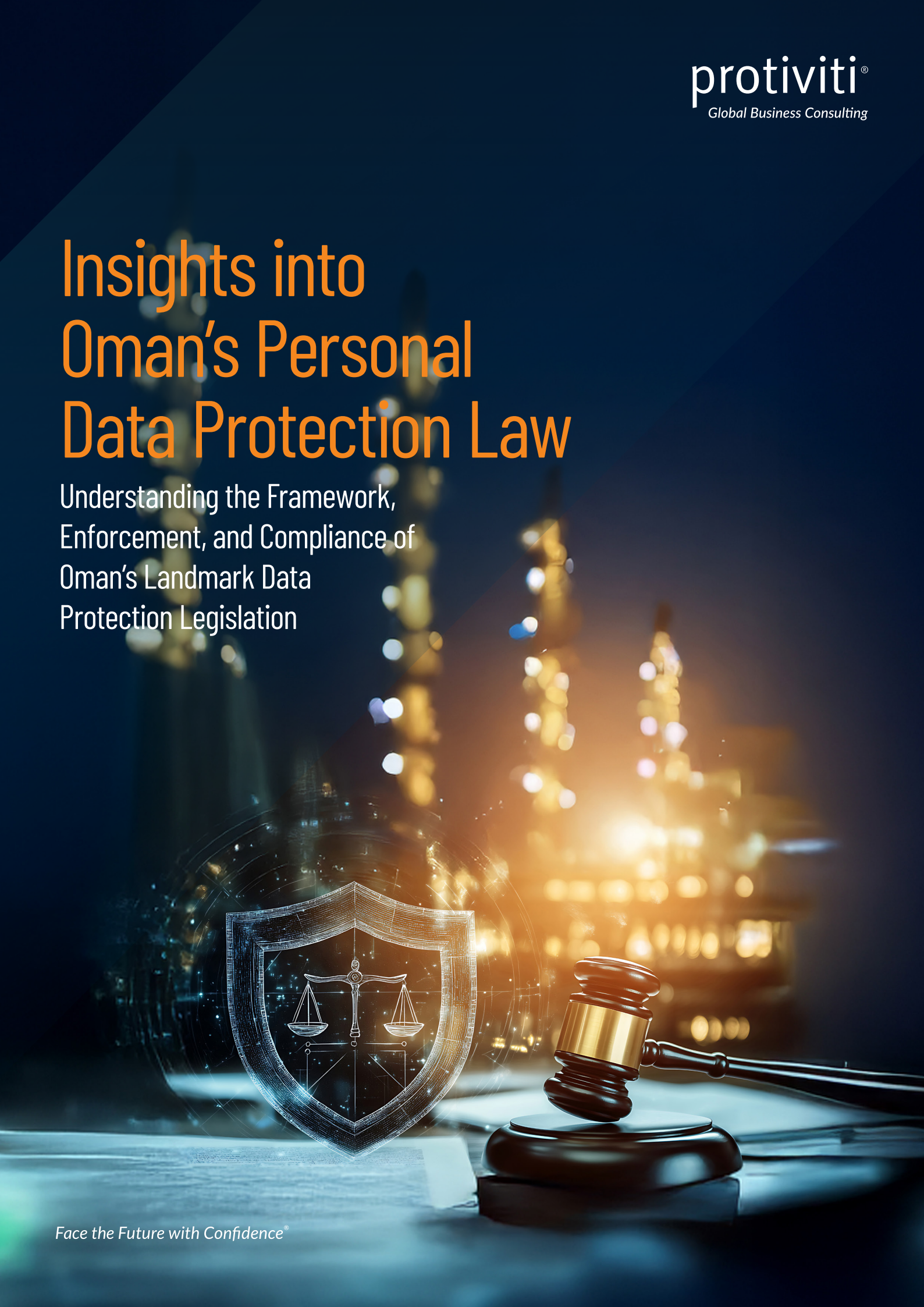
protiviti®
Global Business Consulting

Insights into Oman's Personal Data Protection Law

Understanding the Framework, Enforcement, and Compliance of Oman's Landmark Data Protection Legislation



Face the Future with Confidence®

Table of Contents

Introduction

The Oman Personal Data Protection Law (PDPL) marks a major advancement in protecting individuals' rights and ensuring accountability in personal data processing in Oman. At a time where organizations are increasingly moving towards achieving Oman Vision 2040 digital transformations and smart infrastructures, the PDPL provides a comprehensive framework that strengthens trust, enhances accountability, and aligns the nation with global privacy and data protection trends.

Compliance with Oman PDPL is necessary to:

- Build customer Trust
- Strengthen the organization's brand value
- Enhance competitive advantage
- Optimize data breach handling
- Support innovation

In this document, we outline a systematic approach and understanding for complying with Oman PDPL. Our methodology integrates a wide range of legal and regulatory expertise with practical implementation experiences ensuring that compliance with data privacy laws becomes part of the organization's DNA.

Law Overview and Execution Roadmap

The Sultanate of Oman has established the Personal Data Protection Law (PDPL) under **Royal Decree No. 6/2022**, published in the Official Gazette on **13 February 2022**. This comprehensive law replaced earlier data protection provisions found in the Electronic Transactions Law and officially came into force on **13 February 2023**. Oversight and enforcement authority are handled by the **Ministry of Transport, Communications and Information Technology (MTCIT)**, reflecting the government's commitment to safeguarding personal data in a rapidly evolving digital landscape. To support implementation of the PDPL, Executive **Regulations** were issued under **Ministerial Decision No. 34/2024**, effective from **5 February 2024**. In January 2024, the Ministry extended the compliance deadline to

5 FEBRUARY 2026

through Ministerial Decision No. 6/2025, offering organizations additional time to align with the law's requirements while maintaining regulatory clarity.

The following article draws on the PDPL, enacted in February 2022 and incorporates the Executive Regulations introduced in February 2024.

Scope of PDPL

- The Law applies to **all processing of personal data**.
- **"Personal data"** means any information that directly or indirectly identifies a natural person, including through:
  - **Identifiers** such as names, civil identity numbers, electronic identifiers, or spatial/location data;
  - **Attributes** related to a person's genetic, physical, mental, psychological, social, cultural, or economic identity.
- **The Law does not limit its scope by industry, method of processing, or source of data. Accordingly:**
  - **All categories of personal data**, including contact, health, and financial data, are covered.
  - **All sources of personal data**, whether provided directly by individuals or obtained from third parties, are included.
  - **All forms of personal data**, whether electronic or paper-based, structured or unstructured, fall within the scope of the Law.

Note: *This description of the scope is an interpretation of the PDPL, as the law itself only states that it applies to the processing of personal data.*

Exclusions Under the Law

The PDPL provides specific circumstances where its requirements do not apply. These exclusions are designed to balance the protection of individual privacy rights with national, legal, and broader societal interests. Accordingly, the PDPL does not apply in the following cases:

- To protect **national security or public interest**.
- Processing carried out by **state bodies or public entities** as part of their legally mandated duties.
- To meet a **legal obligation**, court judgment, or official decision.
- To protect the **economic or financial interests** of the State.
- To protect the **vital interests of the data subject**.
- For **crime detection or prevention**, based on a formal request from the competent investigation authorities.
- To **execute a contract** to which the data subject is a party.
- Processing carried out within the **personal or family sphere**.
- Processing for historical, scientific, literary, statistical, or economic research purposes, provided that individuals cannot be identified in the published results.
- Processing of personal data that is **publicly available**, where such use does not conflict with the provisions of the PDPL.

Fines Under the Law

The PDPL is established with the purpose of ensuring accountability and compliance. The MTCIT is empowered to impose administrative penalties on organizations that violate the provisions of the PDPL or its Executive Regulations. These penalties include:

- **Official warning** – A formal notice issued in response to non-compliance.
- **Suspension of authorization** – Temporarily applied pending rectification of the violation.
- **Administrative fines** – Monetary penalties of up to OMR 2,000 (two thousand Omani Rials) for each violation.
- **Revocation of authorization** – Permanent in cases of severe or repeated non-compliance.

Penalties Under the Law

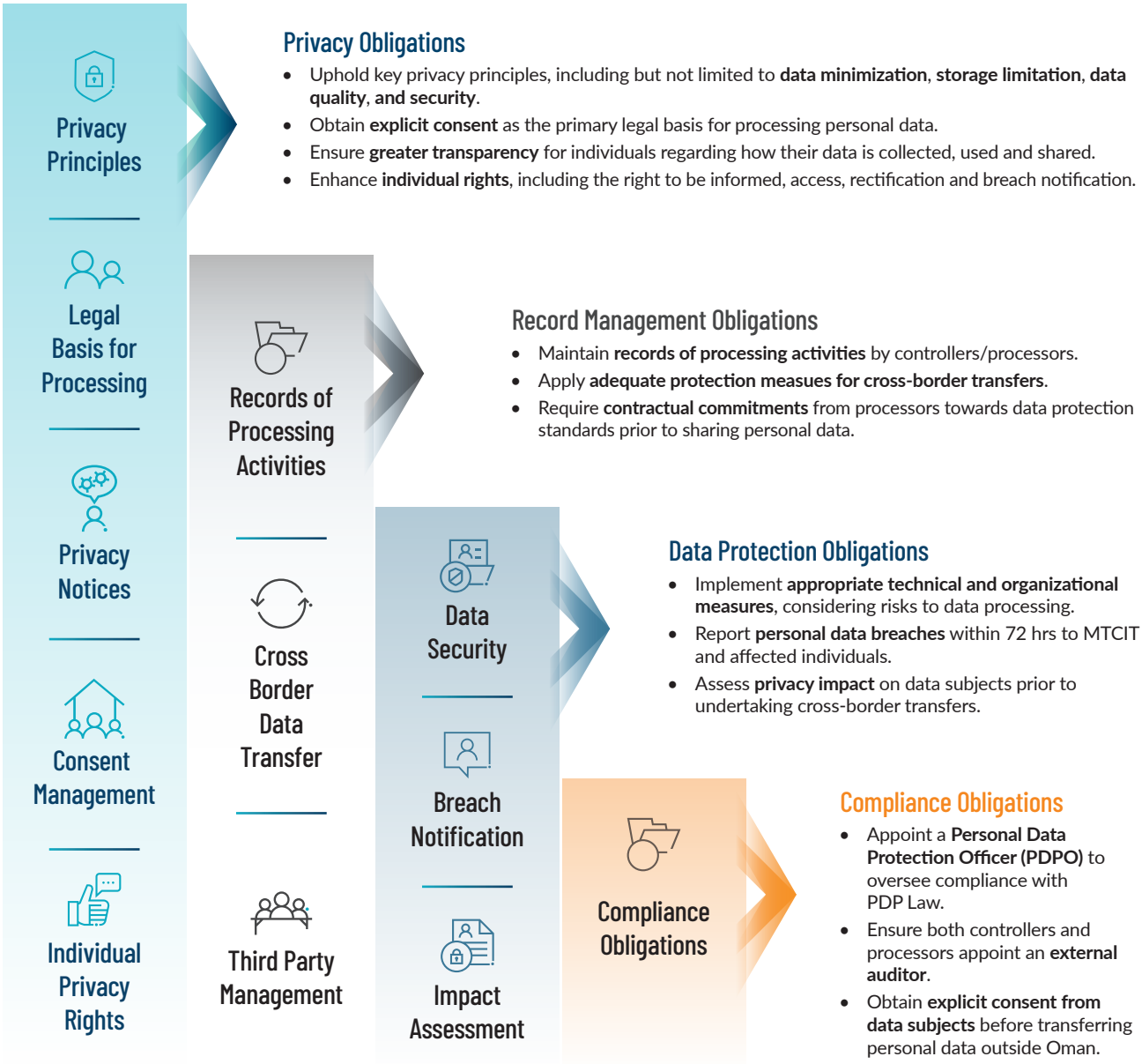
Violations of the Law may result in penalties ranging from **OMR 500 to OMR 500,000**, depending on the specific provision breached, with higher penalties applying to serious violations such as unlawful cross-border transfers or breaches involving legal persons.

Core Elements of Law

The key requirements of the PDPL cut across various areas, including risk management, compliance, legal obligations, data protection, data governance, and records management, ensuring responsible and transparent handling of personal data.

Importantly, the PDPL reflects global best practices in data protection, aligning Oman with international standards of privacy and trust while being tailored to the national context. For organizations, this calls for a holistic, structured, and collaborative approach to be adopted to establish robust privacy programs that enhance digital trust, support innovation, and reinforce competitiveness in an increasingly data-driven economy.

Fundamental Obligations Under the Law



Privacy Obligations

- Uphold key privacy principles, including but not limited to **data minimization**, **storage limitation**, **data quality**, **and security**.
- Obtain **explicit consent** as the primary legal basis for processing personal data.
- Ensure **greater transparency** for individuals regarding how their data is collected, used and shared.
- Enhance **individual rights**, including the right to be informed, access, rectification and breach notification.

Record Management Obligations

- Maintain **records of processing activities** by controllers/processors.
- Apply **adequate protection measues for cross-border transfers**.
- Require **contractual commitments** from processors towards data protection standards prior to sharing personal data.

Data Protection Obligations

- Implement **appropriate technical and organizational measures**, considering risks to data processing.
- Report **personal data breaches** within 72 hrs to MTCIT and affected individuals.
- Assess **privacy impact** on data subjects prior to undertaking cross-border transfers.

Compliance Obligations

- Appoint a **Personal Data Protection Officer (PDPO)** to oversee compliance with PDP Law.
- Ensure both controllers and processors appoint an **external auditor**.
- Obtain **explicit consent from data subjects** before transferring personal data outside Oman.

What Should Companies Do?

The PDPL represents a fundamental shift in how organizations must approach the collection, processing, and management of personal data. Its impact spans all sectors that handle personal information, requiring businesses to move beyond reactive compliance toward proactive personal data governance.

The following section outlines key considerations and practical steps to help organizations effectively navigate their PDPL compliance journey and align their policies, processes, and controls with the data protection requirements while building trust in a data-driven economy.

Visibility Over Personal Data

With digital adoption on the rise in Oman, organizations are processing more personal data than ever. The PDPL and its Executive Regulations impose strict duties on data controllers and processors, from honoring individual rights to safeguarding sensitive data like health and children's information.

To stay compliant, businesses need clear visibility into how personal data moves through their systems. This starts with a thorough data discovery and mapping exercise identifying where data is collected, stored, processed, and shared. That clarity is key to building a privacy program that meets legal standards and earns public trust.

Consent Management

The PDPL recognizes **consent** as a primary lawful basis for processing personal data, requiring organizations to obtain **explicit consent** of data subjects before initiating or continuing processing activities. Equally important, data subjects must be able to **withdraw consent** through mechanisms that are as simple and accessible as the process for providing it.

The Executive Regulations require explicit consent for activities like marketing and advertising. For children's data, consent must come from a legal guardian, and all processing must clearly serve the child's best interests.

To comply, companies should review and strengthen their consent collection and management practices. This includes ensuring that consent is **informed**, **specific**, and **unambiguous**, maintaining robust **records of consent**, and providing clear, accessible and user-friendly **withdrawal mechanisms**.

Upholding Individuals' Privacy Rights

Under the PDPL, individuals are granted **comprehensive rights over their personal data**, empowering them to play an active role in how their information is collected, used, and retained. These rights include the **right to be informed**, **right of access**, **right to correction or rectification**, **right to erasure**, and **right to object to processing**. This means that data subjects can request organizations to provide a copy of their personal data, correct inaccuracies, or delete specific information.

The Executive Regulations require that organizations to **respond to such requests within 45 days**. In some cases, organization may refuse to fulfill the request of the data subject (e.g. if the request is unjustifiably repetitive or its fulfillment requires extraordinary effort).

Addressing Cross-border Transfer Concerns

Cross-border transfers of personal data are tightly regulated under Oman's PDPL. Organizations may only transfer data abroad if the individual has given **explicit consent** and the receiving country or entity offers data protection standards that match or exceed those set by Oman's law. Organizations must also **assess the risks** associated with such transfers before they take place. While no official adequacy list of countries has been published, transfers to jurisdictions that lack equivalent data protection standards require additional safeguards to ensure compliance.

Companies with a global footprint should carefully review their **data transfer practices**, **conduct risk assessments**, **implement adequate technical and organizational safeguards**, and maintain documentation to demonstrate that all cross-border data transfers comply with the PDPL.

Use of Third Parties

Under the PDPL, controllers remain fully accountable for personal data shared with third-party processors. Organizations must therefore adopt a rigorous approach to vendor management to ensure compliance. Before engaging vendors, companies must:

Under the PDPL, organizations that engage third-party processors remain fully responsible for how personal data is handled. This means companies must take a proactive and structured approach to managing external vendors who process data on their behalf.

- Evaluate the vendor's data protection practices and security posture through detailed due diligence.
- Put in place binding agreements that clearly outline the scope of processing, confidentiality terms, security expectations, and breach reporting protocols.
- Seek prior approval for any subcontracting arrangements to maintain oversight and transparency.
- Regularly assess vendor performance and compliance through audits or periodic reviews.
- Maintain clear lines of accountability with the MTCIT, recognizing that while processors must report breaches, the controller bears ultimate responsibility for ensuring lawful and secure data handling.

Specific Obligations for Data Controllers

Under the PDPL, data controllers—organizations that determine the purposes and means of personal data processing—bear the primary responsibility for ensuring compliance with the law and its Executive Regulations. Controllers must adopt a proactive, risk-based approach to data protection, embedding accountability throughout their operations.

Key obligations include:

- **Cooperation with the MTCIT**: The Controller must cooperate with the Ministry by providing the necessary data and documents on request.
- **Engage an external auditor**: Upon the Ministry's request, the Controller must appoint an external Auditor to assess compliance. The auditor's findings must be formally submitted to the Ministry.
- **Lawfulness, fairness and transparency**: All data activities must be based on a valid legal ground such as explicit consent and clearly communicated to individuals.
- **Data security**: Implement strong technical and organizational controls to prevent unauthorized access, misuse, or loss of personal data.
- **Records of Processing Activities (ROPA)**: Keep detailed documentation of processing operations, including data types, purposes, retention timelines, recipients, and any international transfers.
- **Governance and oversight**: Designate a Personal Data Protection Officer (PDPO) and work with an approved external auditor to oversee compliance and provide independent assurance.
- **Processor management**: Ensure that any external processors operate under strict contractual terms, follow documented instructions, and uphold all PDPL requirements.
- **Data subject rights management**: Effectively manage data subject rights by ensuring timely responses to requests for access, correction, erasure, objection, and withdrawal of consent.
- **Breach notification**: Reporting personal data breaches to the MTCIT within the mandated 72-hour timeframe, and where the breach is likely to cause serious harm or high risk to affected individuals, they too must be informed to the affected individuals within the same timeframe, along with details of the incident and steps taken to contain or mitigate its impact.

Data Processor Obligations

Under PDPL, processors handling personal data on behalf of controllers must operate within strict legal and contractual boundaries. Although controllers hold overall responsibility, processors are independently accountable for maintaining data protection standards and supporting compliance efforts.

Key obligations include:

- **Engaging with MTCIT**: Processors are required to cooperate with the MTCIT by furnishing relevant records and documentation when requested.
- **Appointment of external auditor**: Upon MTCIT's request, the Processor must appoint an external auditor to verify compliance with processing procedures and controls. A copy of the auditor's report must be provided to MTCIT.
- **Lawful processing on instructions**: Process personal data strictly in accordance with the documented instructions of the controller and refrain from processing for any unauthorized purposes.
- **External Auditor**: Upon MTCIT's request, the Processor must appoint an external auditor to verify compliance with processing procedures and controls. A copy of the auditor's report must be submitted to MTCIT.
- **Records of Processing**: They must keep detailed logs of all processing carried out for controllers, including the types of data involved, the purpose of processing, recipients, and any cross-border transfers.

Breach Notification

Under the PDPL, organizations must report any personal data breach to **MTCIT within 72 hours of discovery**, if the incident poses a risk to the privacy, confidentiality, or security of individuals. If the breach is likely to result in **serious harm or a high risk** to individuals, the affected data subjects must also be informed without undue delay, generally within the same 72-hour period. The Executive Regulation provides guidance on the criteria for reporting breaches and communicating with data subjects.

In light of these requirements, organizations should review and strengthen their **security monitoring and incident management programs** to ensure early detection of potential breaches. Incident management processes should be **integrated with privacy oversight**, and procedures should be clearly defined to ensure **timely and compliant breach notifications** under the PDPL.

Appointment of Personal Data Protection Officer (PDPO)

Under the PDPL, **data controllers** are required to designate a Personal Data Protection Officer (PDPO) responsible for governing and overseeing the implementation of the organization's personal data protection program and ensuring compliance with the PDPL and its Executive Regulations.

Both controllers and processors are required by MTCIT to appoint an external auditor for reviewing compliance, evaluating safeguards, and submitting periodic reports to MTCIT.

In addition to these formal roles, organizations should build a structured Data Privacy Program to manage personal data responsibly and consistently. Key elements of such a program include:

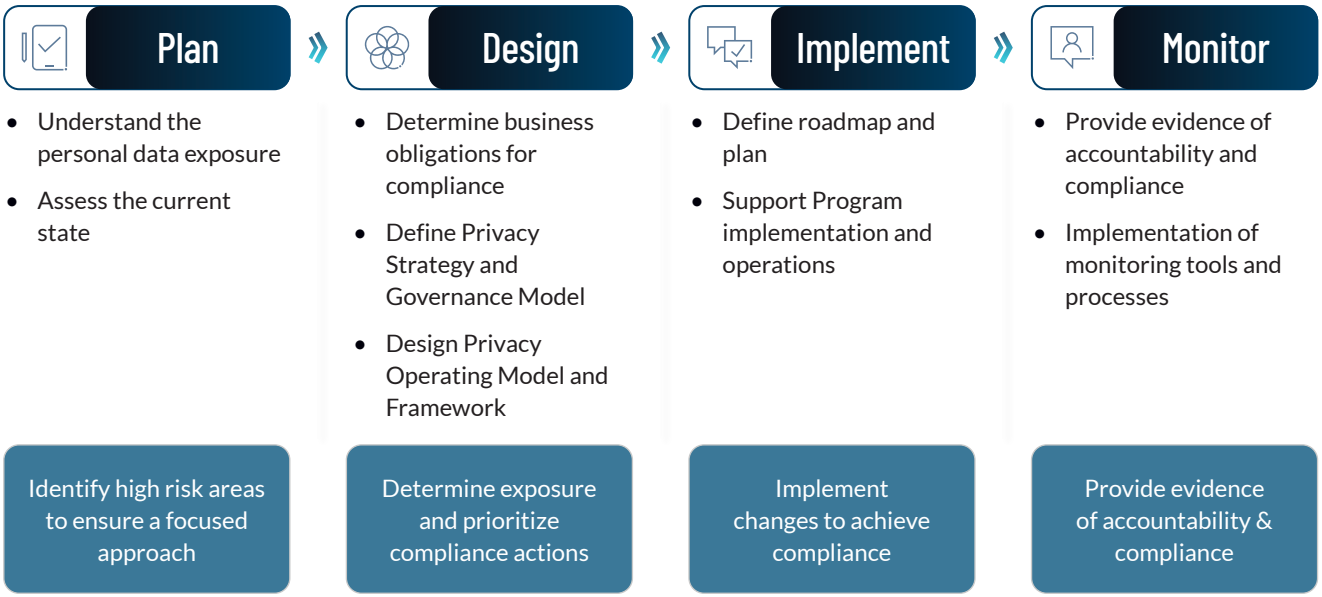
- Setting up governance frameworks to identify and manage privacy risks.
- Creating and updating internal policies and procedures that reflect legal obligations.
- Defining clear roles and accountability for data protection across teams.
- Integrating privacy and risk management into day-to-day data handling practices.

By embedding these practices, companies can establish a resilient compliance model that meets regulatory expectations and builds long-term trust with customers, partners, and regulators.

How Can Protiviti Support?

Protiviti supports organizations in navigating their compliance journey with the PDPL through a structured, yet flexible, phased approach. This methodology is tailored to address client-specific needs while ensuring full alignment with regulatory obligations. Our approach is organized into four key phases, guiding organizations from initial assessment to implementation and ongoing monitoring.

By leveraging this framework, Protiviti has successfully assisted numerous clients in establishing and enhancing their privacy programs, enabling them to not only achieve compliance but also foster lasting trust with their stakeholders.



Duration of each phase and level of effort is highly dependent on personal data processed, the size and scope of organization'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, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Contacts

Shatha Al-Maskiry
Managing Director
+968 99848584
Shatha.Maskiry@protivitiglobal.me

Niraj Mathur
Managing Director
+971 502547507
Niraj.Mathur@protivitiglobal.me

Dr. Abdullah Al Balushi
Managing Director
+968 9203 0305
Abdullah.Albalushi@protivitiglobal.me

Our Offices in the MENA

Abu Dhabi
Emirates Real Estate Corporation
Building, 7th Floor, Office 707-711
Al Falah Street, Al Danah,
P.O. Box 32468, Abu Dhabi, UAE

Bahrain
Platinum Tower, 17th Floor
P.O. Box 10231, Diplomatic Area
Manama, Kingdom of Bahrain

Dubai
Office No. 2104, 21st Floor
U-Bora Tower 2, Business Bay
P.O. Box 78475, Dubai, UAE

Egypt
Cairo Complex
Ankara Street Bureau 1
First Floor, Sheraton Area
Heliopolis - Cairo, Egypt

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al Waleed Street, Sharq
P.O. Box 1773, Safat 13018, Kuwait

Oman
Al-Ufuq Building, 2nd Floor
Office No. 26, Shatti Al Qurum
P.O. Box 1130, P.C. 112
Ruwi Muscat, Oman

Qatar
Palm Tower B 19th Floor
P.O. Box 13374, West Bay
Doha, Qatar

Saudi Arabia - Dammam
Q1-5, The Business Quarter
Salman Al Farisi St,
Al Khalidiyyah Al Janubiyyah,
Dammam, Eastern Province, 32221,
Kingdom of Saudi Arabia

Saudi Arabia - Jeddah
King Abdulaziz Branch Road
Ash shati district , Building No. 7524
P.O. Box 3675, Jeddah 23412
Kingdom of Saudi Arabia

Saudi Arabia - Riyadh
Al-Ibdaa Tower, 9th & 18th Floor
King Fahad Branch Road, Al-Olaya,
Building No. 7906, P.O. Box 3825
Riyadh 12313, Kingdom of Saudi Arabia

Face the Future with Confidence®

149273_OCT2025