Deloitte | A Middle East Point of View - Summer 2025 | Data protection

Transforming your business: Uncovering the missing pieces in KSA Personal Data Protection Law compliance

The missing piece

Months after the compliance deadline for the Personal Data Protection Law (PDPL) set by the Saudi Data & AI Authority (SDAIA), its impact is becoming increasingly evident. Organizations based in the Kingdom of Saudi Arabia are striving to meet the law's requirements and, as a result, are investing in multiple privacy compliance-oriented projects.

Some organizations are placing a strong focus on establishing robust governance frameworks, prioritizing the development and formalization of privacy policies, procedures, and operational guidelines. This includes drafting and publishing privacy notices, deploying consent forms, and setting clear protocols for managing Data Subject Rights (DSR) and personal data breaches.

In fact, some organizations are taking compliance to the next level by automating consent tracking, rights request management, and privacy notices. These efforts help increase maturity levels and offer a growing sense of confidence that compliance is well in hand.

While the measures implemented through various privacy projects are essential and highly visible to both regulators and Data Subjects, a critical blind spot still remains.

The missing piece lies within the name itself: the Personal Data Protection Law—a framework that embodies the true essence of safeguarding and protecting personal data.

Article 19 of the PDPL clearly outlines the obligation to apply the necessary organizational and technical measures to protect personal data from loss, damage, unauthorized access, or disclosure. This aspect of compliance is less flashy, more technical, and often more complex to implement—yet it is fundamental to ensuring effective personal data protection.

Addressing some missing pieces

1. Lack of privacy access rights reviews

Many organizations conduct periodic access rights reviews from a cybersecurity perspective, covering the fundamental principles of confidentiality, integrity, and availability (CIA). However, these reviews often overlook who has access to personal data. Understanding the distinction between a regular access rights review and a privacy-specific access rights review is crucial for effective privacy governance and compliance under regulations such as the PDPL.

The following highlights the key differences:

Regular access rights review

- Regularly conducted by the Information Technology (IT) department, Information Security department, or department managers
- Focuses on all types of data and doesn't always distinguish between the various types (e.g., financial, personal, or business-related)
- Often aligns with internal policies or IT governance
- Access is granted based on user group or role

Privacy access rights review

- Regularly conducted by the Data Protection Officer (DPO) and assisted by the business owner
- Focuses on users and roles with access to personal data
- Often aligns with privacy policy
- Access is granted based on the lawful basis of processing, purpose limitation, or need-to-know basis

2. Missing personal data classification

Most organizations adopt the data classification standard published by National Data Management Office (NDMO) and implement it across all their data. However, personal data is often treated as regular data, resulting in a failure to correctly classify it within systems and applications. Without a proper classification framework that takes personal data into consideration, it becomes challenging to apply proportional protection measures through Data Leakage Prevention (DLP), Mobile Device Management (MDM), and other technical solutions in a proportionate and effective manner.

DLP systems can identify the types of data being processed—such as names, ID numbers, and email addresses. However, they often lack context regarding how or why the data was collected, especially in cases where it originated from public sources or was collected with user consent.

To overcome this, organizations should enable DLP systems to apply appropriate rules based on contextual factors such as data source and consent. In addition to that, Data Classification tools should be configured to classify data during ingestion or creation, using labels that reflect how the personal data was collected. Examples include:

- Personal Data – Consent
- Personal Data – Public Source
- Sensitive Personal Data – Contractual

These tags would be stored with the data and remain consistent across systems (structured or unstructured).

3. Inadequate Generative Artificial Intelligence (GenAI) and robotics controls

Most organizations are rapidly adopting GenAI tools like ChatGPT and Microsoft Copilot to enhance productivity and automate tasks. In doing so, employees often upload sensitive information such as personal data, HR records, or internal documents leading to unauthorized data sharing, data breaches, and regulatory non-compliance. To address this issue, organizations should implement distinct sets of technical requirements, procedures, and processes, such as:

- **Internal GenAI policy and usage guidelines:** Train employees to avoid uploading identifiable personal data unless the tool has been approved for such use.
- **Consent management for AI interactions:** Ensure explicit, informed consent is obtained when AI tools interact with Data Subjects (e.g., during Data Subject Rights requests or when handling Data Subject queries).
- **Privacy by design:** Ensure these systems are designed with privacy by default. This includes data retention limits, masking, and user-level access control.
- **DLP integration with Next-Gen Firewalls (NGFWs):**
  - Inspect outbound traffic (HTTPS/SSL) to identify sensitive data (e.g., personal data, protected health information (PHI), and payment card data (PCI) in real-time).
  - Block or alert when specific patterns (e.g., national ID, email addresses, payroll data) are being sent to specific cloud domains or APIs (e.g., chat.openai.com, api.openai.com, or copilot.microsoft.com).
  - Enforce policy-based restrictions (e.g., allow only anonymized data or prevent upload of any HR or financial records).

4. Inadequate technical safeguards

Organizations typically implement technical controls based on National Cybersecurity Authority - Data Cybersecurity Controls (NCA-DCC), National Cybersecurity Authority - Essential Cybersecurity Controls (NCA-ECC), and international cybersecurity standards and best practices. However, personal data is frequently treated as regular data, with standard security controls applied uniformly across all data types.

Below are common areas that are often overlooked when implementing appropriate personal data technical safeguards:

- Encryption of personal data (at rest and in transit)
- Monitoring and auditing of access and usage of personal data
- Running vulnerability assessments for systems that store and process personal data
- Updating incident response processes specific to personal data breaches

Most organizations adopt the data classification standard published by National Data Management Office (NDMO) and implement it across all their data. However, personal data is often treated as regular data, resulting in a failure to correctly classify it within systems and applications.

Outside the box

Choosing the right privacy and protection practitioner

Selecting the right privacy and protection practitioner is crucial. Many practitioners treat the data privacy function in silo, failing to oversee and incorporate it effectively within the existing functions of an organization. A key principle that privacy practitioners, especially those advising organizations in the Kingdom of Saudi Arabia, should consider is the importance of thinking outside the box.

For example, there is the right to request destruction of personal data. The PDPL gives individuals the right to request destruction, hence the erasure of their personal data. This applies to all copies of their data, including those stored in backups. However, SDAIA recognizes that it is technically impractical to immediately delete specific data from permanent backups (e.g., full-image backups or tapes). Nevertheless, if or when a backup is restored, any previously deleted personal data must also be re-deleted as part of the restoration process.

In addition, organizations should:

- **Document the limitation:** Policies and privacy notices should clearly state that while Right to Request Destruction requests are executed promptly in live systems, deleted data may remain in backups until those backups expire or are overwritten.
- **Ensure no restoration without controls:** Procedures should be in place to ensure that, following the restoration of a backup, all deletion requests processed since the backup was made.

Deloitte | A Middle East Point of View - Summer 2025 | Data protection

What organizations should do

- **Build or strengthen their Data Classification Framework:** Clearly define and label personal data within all systems, and link classification to handling rules.
- **Conduct regular privacy access reviews:** Set up processes (automated where possible) to review access rights to personal data at regular intervals and ensure role-based and privileged access control is enforced through Identity Access Management (IAM) solutions.
- **Harden technical protections:** Invest in core data security measures, encryption, monitoring, DLP, and secure development practices for applications processing personal data.
- **Ensure end-to-end lifecycle protection:** From collection to deletion, apply strict controls on how personal data is stored, shared, and ultimately destroyed.
- **Data Protection Officer (DPO):** Oversee data privacy and protection practices, conduct regular privacy risk assessments, and coordinate with regulators.
- **Privacy awareness and training programs:** Continuous awareness sessions and training programs empower employees, reduce human error, and build a culture of accountability and data responsibility across an organization.
- **Privacy by Design (PbD):** Ensures that data protection is built into systems, processes, and technologies from the beginning, reducing risks, ensuring compliance, and safeguarding personal data by default.
- **Data Security Posture Management (DSPM):** Provides organizations with continuous visibility into where sensitive and personal data resides, whether on-premises or across cloud environments. Helps identify data stores, classify personal data, detect misconfigurations or unauthorized access, and enforce security policies, which would proactively reduce privacy risks, ensure compliance with data protection regulations, and strengthen their overall ability to protect personal data against leaks, misuse, or breaches.

Achieving PDPL compliance requires more than well-written policies and automated consent tools. At the core of data privacy is data protection, which means embedding robust technical and organizational controls into every layer of the data ecosystem. Organizations that focus solely on the visible aspects of compliance risk missing out on the deeper obligations that truly secure personal data, ultimately falling short of the law's true intent.

By **Carlos Obeid**, Data Protection Senior Manager and **Daniel Brierley**, Partner, Cyber – Digital Trust and Privacy and, Deloitte Middle East