FAQs | PDPL compliance in SAP landscapes

The Kingdom of Saudi Arabia's Personal Data Protection Law (PDPL) came into effect in September 2023, marking an important step in aligning Saudi Arabia's data privacy framework with global standards.

1. How does PDPL affect SAP HCM and SuccessFactors data?

PDPL applies to all personal data, including employee records in SAP HCM and SuccessFactors. Organisations must carefully manage sensitive information such as identification numbers, salaries and contact details across Production, non-production systems. Compliance requires anonymisation*, pseudonymisation*, and secure access controls.

Anonymised data can't be traced back to a real person, while pseudonymised data can still be linked back if someone has access to the additional information- so it still carries risk and must be protected accordingly.

2. What are the biggest PDPL risks in SAP non-production environments?

Non-production systems often contain full copies of Production data. Without masking* or scrambling*, these environments can expose sensitive employee or customer information. Organisations need strategies to ensure non-production systems do not contain identifiable personal data, while still supporting development and training activities.

3. How can SAP customers enforce PDPL data retention policies?

SAP landscapes often accumulate historical personal data across multiple modules. PDPL requires that organisations retain data only as long as necessary. This involves implementing retention schedules, automated archiving or deletion, and audit logs to demonstrate compliance during internal reviews or regulatory inspections.

4. How does PDPL impact SAP cross-system integrations and data transfers?

PDPL restricts the transfer of personal data outside Saudi Arabia unless specific legal conditions are met. This affects integrations between SAP S/4HANA, SuccessFactors, Concur, and other third-party systems. Organisations must ensure data flows are secure, localised, and compliant without disrupting operational processes.

5. What steps should I take to secure SAP analytics and AI data under PDPL?

Analytical and AI systems often require aggregated personal data. Compliance requires that sensitive data is pseudonymised* or masked before being used in analytics. This allows AI and reporting processes to remain effective while reducing privacy risks.

6. How can business users manage PDPL compliance in SAP without heavy IT involvement?

PDPL compliance is easier with role-based access, approval workflows, and consent tracking. HR, finance, and operations teams can manage who sees and uses data directly in SAP, reducing the need for IT and speeding up compliance.

7. How can I audit PDPL compliance across SAP landscapes?

PDPL requires organisations to demonstrate accountability. In SAP environments, data is often spread across multiple modules. Auditing involves identifying where personal data resides, who has access, and which measures are in place to protect it. Audit reports provide evidence for internal checks and regulatory requests.

8. What SAP-specific approaches support PDPL-compliant data masking or anonymisation?

Approaches include:

- Masking or pseudonymising sensitive data during system copies.
- Securing Test, QA, and Sandbox environments.
- Enforcing access controls and monitoring data usage.
- Applying retention and archiving strategies across modules.

These steps help protect data at rest, in transit, and during processing.

9. How do PDPL requirements differ from GDPR for SAP customers in Saudi Arabia?

While PDPL and GDPR share privacy principles, PDPL has unique localisation, consent, and retention requirements. SAP customers must adapt GDPR-based processes to meet local rules, including keeping data within Saudi borders unless legal exemptions apply, and complying with local regulatory guidance.

Anonymisation: The process of permanently removing or altering personal data so that an individual can no longer be identified.

Pseudonymisation: The process of replacing identifiable information with artificial identifiers or codes, while still allowing the data to be re-identified if additional information (kept separately and securely) is used.

Masking: The process of hiding or transforming sensitive data so that it becomes unreadable or unusable to unauthorised users, while still looking realistic enough for testing or training purposes. Masking protects real data by replacing it with safe, non-identifying values.

Scrambling: The process of randomly rearranging or altering characters within a data field so the original information becomes unreadable and cannot be easily reconstructed. It's a form of data masking that keeps the data format intact but removes any meaningful value.

epiuselabs.com | info@labs.epiuse.com

James Watson

SAP Landscape and Data Management Specialist, EPI-USE Labs

james@labs.epiuse.com

Rohin Ramjee

SME Security & Data Privacy Lead at EPI-USE Labs

rohin.ramjee@labs.epiuse.com