Saudi Arabia Data Protection Health Check

Governance and Accountability	✓
Do you have a designated Data Protection Officer (DPO) where required, and are their contact details accessible to data subjects and the competent authority?	
Is your organisation registered on the National Data Governance Platform, and is your registration up to date?	
Do you have a documented data protection governance model, including clear roles and responsibilities for data privacy across the organisation?	
Are regular internal or external compliance assessments conducted to verify adherence to the PDPL?	

Data Processing Principles	✓
Are personal data collected for specified, explicit, and lawful purposes, and are these purposes documented?	
Is the amount of personal data collected limited to what is strictly necessary for the stated purposes (data minimisation)?	
Are data processing activities regularly reviewed to ensure ongoing relevance and necessity?	
Are there procedures in place to ensure the accuracy, completeness, and currency of personal data?	

Privacy Notices and Transparency	✓
Do you provide clear and accessible privacy notices to data subjects, informing them of the legal basis and purpose for data collection and processing?	
Are data subjects informed of their rights under the PDPL, including the right to access, correct, update, or erase their data?	
Are privacy notices updated regularly and made available through appropriate channels (e.g., website, app, email)?	

Data Subject Rights	✓
Do you have documented procedures for data subjects to exercise their rights (access, correction, erasure, withdrawal of consent, etc.)?	
Are requests from data subjects handled within the timeframes specified by the PDPL?	
Are data subjects able to easily access and obtain copies of their personal data?	

Consent Management	✓
Is consent obtained where required, and is it recorded and stored appropriately?	
Are consent requests clear, distinguishable from other terms, and written in plain language?	
Can data subjects withdraw their consent at any time, and is the withdrawal process straightforward?	

Legal Bases for Processing	✓
Are all data processing activities mapped to a valid legal basis under the PDPL (e.g., consent, contractual necessity, legitimate interest, legal obligation)?	
Is sensitive data processed only with explicit consent or as otherwise permitted by law, and are additional safeguards in place?	

Data Processors and Third Parties	✓
Are there policies and procedures for selecting and managing data processors and sub-processors, ensuring they provide adequate data protection guarantees?	
Are data processing agreements in place with all processors, specifying roles, responsibilities, and security measures?	
Are third-party disclosures and data sharing documented and justified under the PDPL?	

Data Retention and Destruction	✓
Are retention periods for each category of personal data defined and documented?	
Is personal data securely destroyed or anonymised once it is no longer necessary for the purpose for which it was collected?	
Are regular audits conducted to identify and delete unnecessary or outdated data?	

Security Measures	✓
Have appropriate organisational, administrative, and technical measures been implemented to protect personal data, including during transfer and storage?	
Are there documented policies for data security, including access controls, encryption, and incident response?	
Are employees trained regularly on data protection and security requirements?	

Data Breach Management	✓
Is there a documented procedure for identifying, containing, and reporting personal data breaches?	
Are breaches notified to the competent authority (SDAIA) within 72 hours, and to affected data subjects where required?	
Are breach incidents documented, and are lessons learned incorporated into future prevention measures?	

Data Transfers Outside the Kingdom	✓
Are cross-border data transfers conducted in accordance with the PDPL, using approved mechanisms such as Standard Contractual Clauses or Binding Common Rules?	
Are transfer impact assessments conducted, and are data subjects informed of international transfers where applicable?	
Are additional safeguards in place for sensitive data transferred outside the Kingdom?	

Special Categories of Data	✓
Are there additional controls for processing health data, credit data, or other sensitive categories, including access restrictions and minimisation of processing?	
Are sector-specific requirements (e.g., from the Ministry of Health or Saudi Central Bank) incorporated into internal policies?	

Record Keeping and Documentation	✓
Do you maintain up-to-date records of all personal data processing activities, including purposes, categories of data, recipients, retention periods, and security measures?	
Are these records available for inspection by the competent authority upon request?	

Training and Awareness	✓
Are all employees who handle personal data regularly trained on PDPL requirements, privacy by design, and the consequences of non-compliance?	
Is there a culture of data protection awareness throughout the organisation?	

If you answered **NO** to any of these questions, you may have a compliance exposure. Please contact us.

Ken Wong
Partner
E ken.wong@cms-cmno.com
T +966 54 768 5580

Masha Ooijevaar
Legal Director
E masha.ooijevaar@cms-cmno.com
T +971 58 852 6404