



Data Classification and Personal Data Protection under Saudi PDPL and NCA DCC



Data Classification and Personal Data Protection under Saudi PDPL and NCA DCC

Technical depth: Practitioner · **Practical mode:** Case study

Introduction

Organisations in Saudi Arabia must classify their data, protect personal data under the Personal Data Protection Law PDPL and apply the National Cybersecurity Authority's Data Cybersecurity Controls DCC. Many still hold unclassified data, incomplete processing records and controls that do not match the sensitivity of what they protect, which exposes them to breaches and regulatory findings. This Core Concept course equips managers to classify data by impact, meet PDPL obligations and map DCC controls to each classification level, alongside ISO/IEC 27001 and 27701. Participants leave with a Data Classification and Protection Register for their own organisation.

Course Objectives

- Map an organisation's data holdings and processing activities as the baseline for classification and PDPL compliance
- Classify data sets as Top Secret, Secret, Restricted or Public using the national impact assessment criteria
- Apply PDPL requirements on legal bases, data subject rights, impact assessments and cross-border transfers to real processing scenarios
- Match NCA DCC and ISO/IEC 27002 controls to each classification level, covering labelling, access, encryption, masking and disposal
- Prepare breach response and third-party processing arrangements that meet PDPL notification and contractual duties
- Produce a Data Classification and Protection Register with a prioritised DCC remediation plan

Target Audience

- Data protection officers and privacy managers responsible for PDPL compliance
 - Data management office managers leading data classification programmes
 - Cybersecurity governance and compliance managers applying the NCA controls
 - Records and information managers overseeing retention and disposal
 - Legal, risk and internal audit managers reviewing data protection arrangements
 - Business unit managers who own personal or sensitive data sets
-

Course Outline

Day 1: The KSA Data Protection Landscape and Data Inventory

- KSA Data Protection Ecosystem: PDPL, SDAIA, NDMO and NCA Responsibilities
- PDPL Definitions: Personal Data, Sensitive Data and Credit Data
- Data Lifecycle Mapping from Collection to Destruction
- Record of Processing Activities RoPA Baseline Template
- Current-State Gap Check Against the NCA DCC-1:2022 Scope

Day 2: Classification Policy, PDPL Rules and Control Frameworks

- KSA Data Classification Policy: Top Secret, Secret, Restricted and Public Levels
- Impact Assessment Scale: High, Medium, Low and None
- PDPL Implementing Regulation: Legal Bases, Data Subject Rights and Controller Duties
- NCA DCC-1:2022 Structure and Its Link to the Essential Cybersecurity Controls
- ISO/IEC 27002:2022 Classification, Labelling and Data Masking Controls

Day 3: Classifying and Protecting Data in Practice

- Classification Decision Tree and Impact Rationale Worksheet
- Labelling and Handling Rules Matrix by Classification Level
- Data Protection Impact Assessment DPIA Template under the PDPL
- Privacy Notice and Consent Record Design
- Access Control and Encryption Requirements Mapped to DCC Controls

Day 4: Transfers, Breaches, Disposal and Third Parties

- Cross-Border Transfer Assessment under the SDAIA Personal Data Transfer Regulation
- Personal Data Breach Response and 72-Hour Notification Playbook
- Data Loss Prevention and Masking Rule Design
- Declassification, Retention and Secure Disposal with NIST SP 800-88
- Processor Contract Clauses and ISO/IEC 27701:2025 Controls for Third Parties

Day 5: Case Work and the Classification and Protection Register

- Hospital Case Study: Classifying Patient and Operational Data Sets
 - E-Commerce Case Study: Consent, Transfer and Breach Decisions
 - Data Classification and Protection Register Build
 - DCC Control Remediation Plan Drafting
 - Peer Review Panel and Register Defence
-

Skills You Will Gain

- Data Inventory Management
- Impact-Based Data Classification
- PDPL Compliance Assessment
- Data Protection Impact Assessment
- DCC Control Mapping
- Breach Notification Handling
- Cross-Border Transfer Assessment
- Secure Data Disposal

Why Attend This Course

- Return to work with a Data Classification and Protection Register for your organisation, already tested against peer review
- Defend each classification decision with a documented impact rationale that an assessor can follow
- Know what to do in the first 72 hours after a personal data breach and who must be told
- Compare classification and privacy practice with managers from other sectors facing the same PDPL and NCA requirements

Conclusion

Data protection holds up only when every data set carries the right classification and the controls match it. This course moves from the KSA data protection landscape and a complete data inventory, through the national classification policy, PDPL rules and the NCA and ISO control frameworks, to classifying and protecting data in practice, and then to transfers, breaches, disposal and third parties. The final day brings the material together in a Data Classification and Protection Register that participants take back to their organisation.