Saudi Cyber Security and Data Protection Law (PDPL) Training Course



Ref: #LEG8754

Course Introduction / Overview:

This course provides a comprehensive exploration of Saudi Arabia's legal framework governing cybersecurity and data protection. In an era of rapid digital transformation driven by Vision 2030, understanding and complying with these regulations is paramount for organizational success and resilience. The curriculum delves deep into the core tenets of the Saudi Personal Data Protection Law (PDPL), the Anti-Cybercrime Law, and the regulations set forth by the National Cybersecurity Authority (NCA) and the Saudi Data and AI Authority (SDAIA). As the renowned legal scholar Daniel J. Solove discusses in his seminal work "Understanding Privacy," the principles of data protection are universal, but their application is uniquely local. This course, offered by BIG BEN Training Center, bridges that gap by contextualizing global best practices within the specific legal and business environment of the Kingdom. Participants will move beyond theoretical knowledge to gain practical, actionable insights for developing robust compliance programs, managing data breaches, and navigating the complexities of cross-border data transfers, ensuring their organizations operate securely and legally in the Saudi digital economy.

Target Audience / This training course is suitable for:

- Legal Counsel and In-house Lawyers.
- Compliance Officers and Managers.
- Data Protection Officers (DPOs).
- Information Security and IT Professionals.
- Risk Management and Audit Professionals.
- Chief Information Security Officers (CISOs).
- Human Resources Managers.
- Marketing and Data Analytics Leaders.
- C-Level Executives (CEO, CIO, COO).
- Government and Public Sector Officials.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Telecommunications and Technology.
- Retail and E-commerce.
- Energy and Utilities.
- Government Agencies and Public Sector Entities.
- Consulting and Professional Services.
- Hospitality and Tourism.
- Logistics and Transportation.
- Education Sector.

Target Organizations Departments:

- Legal and Corporate Affairs.
- Compliance and Regulatory Affairs.
- Information Technology (IT) and Information Security.
- Internal Audit and Risk Management.
- Human Resources.
- Marketing and Sales.
- Procurement and Vendor Management.
- Customer Service and Support.
- Research and Development.
- Executive Management.

Course Offerings:

By the end of this course, the participants will have able to:

- Analyze the key provisions of the Saudi Personal Data Protection Law (PDPL).
- Understand the roles and responsibilities of data controllers and processors.
- Develop a framework for managing data subject rights under PDPL.
- Implement the National Cybersecurity Authority's (NCA) Essential Cybersecurity Controls (ECC).
- Navigate the legal requirements of the Saudi Anti-Cybercrime Law.
- Conduct a Privacy Impact Assessment (PIA) tailored to the Saudi context.
- Formulate a legally compliant data breach incident response plan.
- Evaluate the legal implications of cross-border data transfers from Saudi Arabia.
- Establish a robust data governance and compliance program within their organization.
- Advise stakeholders on cybersecurity and data privacy risks and mitigation strategies.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive. We believe that adult learning is most effective when it connects theory to real-world application. This course moves beyond traditional lectures to foster a dynamic learning environment where participants actively engage with the material. The program is built on a foundation of expert-led instruction, where our experienced facilitators break down complex legal concepts into understandable and manageable components. This is complemented by an extensive use of case studies drawn from actual scenarios within the Saudi market, allowing participants to analyze challenges and formulate solutions relevant to their own industries. Interactive group discussions, workshops, and problem-solving sessions encourage collaborative learning and the sharing of diverse perspectives. Participants will work on practical exercises, such as drafting privacy notices and mapping data flows, to build tangible skills. Continuous feedback and Q&A sessions are integrated throughout the course to ensure clarity and reinforce key learning objectives, creating a comprehensive and impactful educational experience.

Course Agenda (Course Units):

Unit One: Foundations of Saudi Cybersecurity and Data Privacy Law

- Introduction to the Saudi Arabian Legal and Regulatory Landscape.
- The Role of Vision 2030 in Driving Digital and Legal Transformation.
- Key Regulatory Bodies: National Cybersecurity Authority (NCA) and SDAIA.
- Overview of the Saudi Anti-Cybercrime Law.
- Core Concepts: Personal Data, Sensitive Data, Processing, and Consent.
- Distinguishing Between Data Privacy and Data Security.
- Global Context: GDPR's Influence on PDPL and Global Data Protection Trends.

Unit Two: The Saudi Personal Data Protection Law (PDPL) in Detail

- Scope and Territorial Application of the PDPL.
- Legal Principles for Processing Personal Data.
- Lawful Bases for Data Processing and Collection.
- Rights of the Data Subject: Access, Correction, Deletion, and Portability.
- Obligations of Data Controllers and Data Processors.
- Requirements for Records of Processing Activities (ROPA).
- Appointing a Data Protection Officer (DPO): Roles and Responsibilities.

Unit Three: Building a PDPL Compliance Framework

- Conducting Data Discovery and Data Flow Mapping.
- Developing and Implementing Privacy Policies and Notices.
- Privacy by Design and by Default Principles.
- Conducting Data Protection Impact Assessments (DPIAs/PIAs).
- Vendor and Third-Party Risk Management Strategies.
- Strategies for Managing Employee Data and HR Compliance.
- Creating a Culture of Privacy Awareness Through Training.

Unit Four: Cybersecurity Regulations and Incident Management

- Deep Dive into the NCA's Essential Cybersecurity Controls (ECC).
- Cybersecurity Governance, Risk, and Compliance (GRC) Frameworks.
- Developing and Implementing an Incident Response Plan.
- Data Breach Notification Requirements under PDPL and NCA Regulations.
- Investigating a Cybersecurity Incident: Forensics and Evidence.
- Communicating with Regulators, Data Subjects, and Stakeholders.
- Legal Liabilities and Penalties for Non-Compliance.

Unit Five: Advanced Topics and Cross-Border Data Transfers

- Regulations Governing Cross-Border Data Transfers from Saudi Arabia.
- Adequacy Decisions and Appropriate Safeguards for Data Exports.
- Legal Considerations for Cloud Computing and SaaS Adoption.
- The Intersection of PDPL with AI and Big Data Analytics.
- E-commerce and Digital Marketing Compliance in the Kingdom.
- Preparing for Regulatory Audits and Investigations.
- Future Outlook: Upcoming Amendments and Trends in Saudi Data Law.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How might the principles of Saudi Arabia's PDPL influence the development of data protection laws in other GCC nations, and what are the implications for regional data-sharing agreements?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself through its singular and deep focus on the Saudi Arabian legal and regulatory ecosystem. While other programs may offer a general overview of global data privacy, this course is meticulously designed to address the specific nuances, obligations, and enforcement realities of the Saudi Personal Data Protection Law (PDPL), the Anti-Cybercrime Law, and the National Cybersecurity Authority's (NCA) frameworks. The curriculum goes beyond mere legal recitation, emphasizing a practical, implementation-oriented approach. Participants learn not just what the law says, but how to translate its requirements into tangible corporate policies, technical controls, and governance structures. We utilize case studies and scenarios that are directly relevant to the Saudi market, addressing the unique challenges faced by organizations operating within the Kingdom. Furthermore, the course uniquely integrates the dual pillars of data privacy (PDPL) and cybersecurity (NCA controls), providing a holistic understanding of digital compliance that is essential for modern risk management. The focus is on building sustainable compliance programs and fostering a resilient security posture that aligns with both legal mandates and the strategic objectives of Saudi Vision 2030.