Jordan PDPL Implementation training Program

Format: (18 Hours Total)
Audience: Interactive workshop, group discussions, Scenarios
Approach: Templates, checklists, forms, Videos

Agenda

Day 1

Module (1): Introduction to the Jordanian Personal Data Protection Law (PDPL)

- Importance of data privacy in the digital era
- Key concepts: personal data, sensitive data, data subject, data controller, processor
- Overview of privacy risks and real-world case studies
- Scope: Who must comply and when
- Regulatory landscape: GDPR and others

Module (2) Legal Basis for Processing Personal Data

- Lawful processing conditions
- Exceptions where processing is permitted without consent
- How to conduct Legitimate interests- real scenarios exercise.

Module (3): Privacy Principles and Data Subject Rights

- The 7 GDPR principles
- Data subject rights under the law
- Responding to subject access requests (SARs)
- How to handle requests and establish workflows

Module (4): Governance, Roles, and Accountability

- Role and responsibilities of Data Protection Officer (DPO).
- Data Controller (المسؤول) vs. Data Processor (المعالج)
- Role of the Data Protection Council (مجلس حماية البيانات)

Day 2

Module 5: Data Mapping and Records

- How to build Records of Processing Activities (RoPA),
- Data inventories and flow mapping.
- Real life exercise.

Module (6): DPIAs and Risk Management

- How to conduct a Data Protection Impact Assessment
- Vendor and third-party data processing
- Real Scenarios Exercises – Full DPIA.

Module (7): Managing Cross-border Transfer

- Managing third-party processors and data sharing
- Data Transfer Impact Assessment form (DTIA)
- Cross-border data transfer rules & safeguards Cross-border transfer checklist
- Scenario.

Day 3 – Advanced Topics & AI in Data Protection

Morning (3 hours)

1. **Cybersecurity & Data Protection**
   - Overlap between data protection & cybersecurity.
   - Phishing, insider threats, weak passwords, and misuse of devices.
   - Secure communication practices (VPNs, encrypted apps, etc.).
   - Case study: Social engineering attack on telecom staff.

2. **Data Protection in AI & Emerging Tech**
   - How AI uses personal data (training data, customer profiling, chatbots).
   - Risks: bias, discrimination, leakage, model inversion.
   - High-level overview: AI in telecom (fraud detection, predictive analytics, customer chatbots) & privacy considerations.
   - International updates: EU AI Act (overview, relation to data protection).

Afternoon (3h)

3. **Best Practices & Organizational Culture**
   - Building a data protection culture.
   - Clear policies, continuous training, and reporting channels.

- "10 Golden Rules" for employees.
- Optional group activity: Spot the data protection mistake in sample scenarios.

4. **Wrap-Up & Final Awareness Session**
   - Recap of key lessons.
   - Role of every employee in protecting data.
   - Q&A session.
   - Distribution of awareness handouts/checklists.

By the end of this 3-day program, employees will:

1. Understand what data protection is & why it matters.
2. Recognize global & local laws and their personal responsibilities.
3. Be aware of telecom-specific risks & compliance obligations.
4. Gain basic awareness of data protection in AI.
5. Learn practical steps to prevent data breaches in their daily work.