Annex (A): Compliance Checklist Template

Applicable to certified external audit firms conducting personal data protection compliance assessments

Item	Compliance Standard	Evidence
Legal Registration	The company must be legally registered in the Sultanate of Oman for at least 12 months and comply with local regulations.	Copy of commercial registration certificate CR 620204 Information Technology and Cyber Security Consulting • Commercial Registration date exceeds 12 months
Certified Qualifications	The company must hold recognized certifications such as ISO/IEC 27001 and ISO/IEC 27701.	• Submit copies of certifications ○ ISO/IEC 27001 ○ ISO/IEC 27701
Technical Team Capability	Lead Auditor must be certified in at least one specialized certification in Information Security and Governance or Privacy and Data Protection.	• Submit list of technical team members and their CVs. • Description of roles (e.g., Project Manager, Lead Auditor) • Lead Auditor certified in at least one of the following Certifications: ○ CCISO (Certified Chief Information Security Officer) ○ CISSP (Certified Information Systems Security Professional) ○ CISA (Certified Information Systems Auditor) ○ CISM (Certified Information Security Manager) ○ ISO/IEC 27001:2022 Lead Auditor ○ CIPP (Certified Information Privacy Professional)
Audit Experience	The company must have proven experience in personal data protection auditing.	• Submit list of previous audit projects • Years of experience

Audit and Documentation Procedures	All audit phases must be thoroughly documented: planning, execution, reporting.	• Audit plan sample covering all three phases (Planning, execution, reporting). Audit report sample
Record Retention	Audit records must be retained for no less than five years.	• Record retention policy • stating minimum 5 years retention period
Legal Compliance	The company must comply with local personal data protection laws.	• Internal policies aligned with laws (e.g., Personal Data Protection Law) • Confirm existence of a compliance unit and designated Data Protection Officer
Data Protection	The company must follow clear procedures to protect data and prevent unauthorized access.	• Internal Data protection policy • Verify implemented security controls (encryption, authorized access, etc.) • Security tests reports (e.g., penetration tests)
Omanization	At least 30% of the technical team must consist of Omani nationals.	• List of technical team members specifying their nationality and job details. • Employment records or contracts demonstrating the required Omanization percentage.