Annex (A): Compliance Checklist

Applies to accredited external auditing firms that will conduct compliance assessments for personal data protection requirements in accordance with the Personal Data Protection Law and its Executive Regulations.

Item	Compliance Standard	Evidence
Legal Registration	The external auditor must hold a valid commercial registration in the Sultanate of Oman, which includes the activity of External Audit in the Field of Personal Data Protection (Activity No. 620209), while complying with all local laws and regulations related to personal data protection.	Copy of • Commercial registration certificate CR. • External Audit in the Field of Personal Data Protection (Activity No. 620209.
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

Annex (A): Compliance Checklist

Applies to accredited external auditing firms that will conduct compliance assessments for personal data protection requirements in accordance with the Personal Data Protection Law and its Executive Regulations.

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.

Annex (B): Compliance Checklist

Applies to accredited external audit firms that will conduct compliance assessments for personal data protection requirements in accordance with the Personal Data Protection Law and its Executive Regulations.

Item	Evidence
Personal Data Protection Policy	A Personal Data Protection Policy document that includes, at a minimum: the rights of the data subject, the methods of data processing, and is placed in a visible location accessible to the data subject.
Data Subject Rights	A document that provides a clear mechanism for obtaining the explicit written consent of the data subject and enabling them to exercise the following rights: • Withdraw their consent to the processing of their personal data, without affecting processing carried out prior to the withdrawal, and request the amendment, update, or restriction of their personal data. • Obtain a copy of their processed personal data. • Transfer their personal data to another controller. • Request the erasure of their personal data, unless such processing is necessary for national archiving and documentation purposes. • Be notified of any breach or violation of their personal data and the actions taken in this regard.
Personal Data Processing Permit	Personal Data Processing Permit According to Article (5) of the Personal Data Protection Law.
Processing of a Child's Personal Data	A document, whether paper or electronic, evidencing the obtaining of explicit consent from the parent or guardian, along with another document demonstrating compliance with the regulations for processing a child's personal data.
Advertising / Marketing / Commercial Materials	A document evidencing the following: • Obtaining the written consent of the data subject. • Notifying the data subject of the means of receiving advertising, marketing, or commercial materials. • Defining the mechanism to stop receiving advertising, marketing, or commercial materials. • Ceasing the sending of advertising, marketing, or commercial materials immediately upon receiving the data subject's opt-out request, free of charge.
Publication / Sharing / Disclosure of Personal Data as	A document evidencing the publication, sharing, or disclosure of personal data as stipulated in Article (5) of the Personal Data Protection Law, in accordance with the legally prescribed limits

Annex (B): Compliance Checklist

Applies to accredited external audit firms that will conduct compliance assessments for personal data protection requirements in accordance with the Personal Data Protection Law and its Executive Regulations.

stipulated in Article (5) of the Personal Data Protection Law:	and cases, or if carried out in execution of a judicial ruling or decision.
Confidentiality of Personal Data:	A document evidencing the following: • Implementation, use, and activation of electronic systems to prevent unauthorized access, leakage, tampering, or misuse of personal data. • Establishment of systems to restore personal data in the event of a physical or technical incident. • Conducting tests to verify the effectiveness of the existing technical measures.
Retention of Personal Data Processing Records:	A document evidencing compliance with the following controls: • The reason for retaining processing records is specific and legitimate. • A retention period is defined that is appropriate to the purpose of the processing. • Technical protection systems are provided to ensure the secure retention of processing records.
Personal Data Breach:	A document detailing the measures and procedures followed before a breach occurs, during the breach, and the corrective actions taken afterward.
Personal Data Protection Officer (DPO):	A document evidencing the designation of the Data Protection Officer (DPO) in accordance with the prepared form, considering the following: • The DPO is qualified to perform the tasks specified in Article (35) of the Executive Regulations, which include: • Providing advice and recommendations to the controller or processor regarding their obligations under the law and regulations. • Monitoring the implementation of the controller's or processor's policies related to personal data protection. • Following up on the controller's or processor's compliance with obligations stipulated by the law and regulations. • Coordinating with the relevant department on matters related to personal data processing.

Annex (B): Compliance Checklist

Applies to accredited external audit firms that will conduct compliance assessments for personal data protection requirements in accordance with the Personal Data Protection Law and its Executive Regulations.

	The data subject must be enabled to contact the Data Protection Officer regarding all matters related to the processing of their personal data.
Transferring Personal Data outside the state:	A document evidencing the explicit consent of the data subject, considering that the transfer or cross-border transfer of data does not compromise national security or the state's higher interests. A document demonstrating that the external data processor has an adequate level of protection for personal data, not less than the level prescribed by the law and regulations, along with a report on the protection level of the external data processor.