DPO Caribbean
Data Protection Risk & Maturity Checklist

Provides insights into how personal data is managed across your organisation

1. Governance & Accountability

☐ Data protection roles and responsibilities clearly defined (e.g., DPO, Privacy Lead, Risk Owners)
☐ DPO appointed (where required) and operating independently
☐ Data protection accountability framework approved by senior management
☐ Regular reporting to executive management / Board
☐ Policies reviewed and approved on a defined schedule

2. Legal Basis & Purpose Limitation

☐ Lawful basis identified and documented for all processing activities
☐ Purposes for processing are clearly defined and communicated
☐ Processing limited to what is necessary and proportionate
☐ Consent mechanisms (where applicable) are valid, documented, and auditable

3. Data Mapping & Records Management

☐ Records of Processing Activities (ROPA) completed and up to date
☐ Personal data flows mapped across systems, vendors, and jurisdictions
☐ Data classification scheme implemented (e.g., personal, sensitive, special category)
☐ Retention schedules defined and enforced

4. Risk Assessment & DPIAs

☐ Privacy risk assessments conducted for new or changed processing
☐ DPIAs completed for high-risk processing activities
☐ Risk mitigation actions documented and tracked
☐ DPO involved in DPIA review and approval
☐ Residual risks escalated and formally accepted where required

5. Data Subject Rights Management

☐ Procedures in place for handling data subject requests (DSARs)
☐ Timelines aligned with applicable regulatory requirements
☐ Identity verification processes implemented
☐ Requests logged, tracked, and auditable

6. Third-Party & Vendor Risk Management

☐ Vendors assessed for data protection and security risk
☐ Data processing agreements in place and reviewed
☐ Cross-border transfer mechanisms documented and lawful
☐ Ongoing vendor monitoring and re-assessment conducted

7. Security & Confidentiality Controls

☐ Technical and organisational security measures implemented
☐ Access controls and role-based permissions enforced
☐ Encryption and secure data transfer mechanisms used where appropriate
☐ Regular testing, vulnerability assessments, and reviews conducted

8. Incident & Breach Management

☐ Personal data breach response plan documented and tested
☐ Clear escalation and notification procedures in place
☐ Breach decision-making and rationale documented
☐ Lessons learned and remediation actions tracked

9. Training & Awareness

☐ Mandatory data protection training provided to staff
☐ Role-based training delivered to high-risk functions
☐ Training completion tracked and refreshed regularly
☐ Awareness materials accessible to employees

10. Monitoring, Audit & Continuous Improvement

☐ Compliance monitoring programme established
☐ Periodic internal audits or reviews conducted
☐ Regulatory changes tracked and assessed
☐ Continuous improvement actions identified and implemented

11. AI & Emerging Technology (Where Applicable)

☐ AI use cases identified and documented
☐ Privacy and ethics risks assessed before deployment
☐ Human oversight and accountability defined
☐ Transparency and explainability considerations addressed