AI Compliance Policy & DPIA Checklist

AI Compliance Policy Template (Mauritius & Southern Africa)

1. **Purpose and Scope** This policy governs the responsible use of AI across operations in Mauritius and Southern Africa. It applies to all business units, employees, contractors, and third-party vendors. 2. **Legal Compliance** - Adhere to Mauritius Data Protection Act (2018), FSC AI Advisory Rules (2021), and HEC AI Guidelines (2025). - Ensure compliance with South Africa POPIA, Zimbabwe Cyber & Data Protection Act (2021), and SADC Model Law (2013). - Apply AU Continental AI Strategy principles for governance and ethics. 3. **Governance and Oversight** - Appoint a Data Protection Officer (DPO) for Mauritius. - Establish an AI Ethics & Compliance Committee. - Maintain an AI Register with model inventory, datasets, risk classification, and owners. 4. **Risk and Transparency** - Conduct Data Protection Impact Assessments (DPIAs) for all high-risk AI systems. - Publish Model Cards, Bias Assessments, and User Disclosures. - Provide human oversight for critical AI decisions (finance, healthcare, education). 5. **Cross-Border Data and Vendors** - Apply adequacy checks and safeguards before transfers within SADC. - Include contractual safeguards (purpose limits, deletion, incident reporting) with vendors. - Prohibit model training on client data without explicit approval. 6. **Monitoring and Review** - Monitor drift, retraining, and security vulnerabilities. - Audit compliance annually and update policies as laws evolve.

Data Protection Impact Assessment (DPIA) Checklist

1. **Description of Processing** - Purpose of AI system - Data categories and sources - Geographic scope (Mauritius, SADC, cross-border transfers) 2. **Legal Basis and Compliance** - Identify lawful basis for processing (consent, contract, legal obligation, etc.) - Verify compliance with Mauritius DPA (2018) and regional laws 3. **Risk Assessment** - Identify potential risks to individuals (bias, discrimination, exclusion) - Assess likelihood and severity of harm 4. **Mitigation Measures** - Data minimization and retention limits - Technical and organizational security measures - Human-in-the-loop controls 5. **Stakeholder Consultation** - DPO review - Consultation with regulators (if required) - Engagement with affected users or communities 6. **Outcome and Sign-off** - Residual risk evaluation - Decision on proceeding, revising, or halting project - Senior management and DPO sign-off