**Regulatory & Data Privacy Compliance Assessment**

*For the Mobile-Based Human Resource Information System (MoHRIS) Project*

**1. Purpose**

To ensure that the MoHRIS system complies with all applicable data protection laws, labor regulations, and industry standards, safeguarding employee data and maintaining legal integrity across all HR operations.

**2. Applicable Legal & Regulatory Frameworks**

| **Jurisdiction** | **Regulation** | **Relevance to MoHRIS** |
| --- | --- | --- |
| **Kenya** | Data Protection Act (2019) | Protects personal and biometric data of employees |
| **Kenya** | Employment Act (2007) | Governs employee recordkeeping, contracts, time tracking |
| **Regional** | EAC Cyberlaws Framework | Cross-border data transfer provisions |
| **International** | ISO/IEC 27001 | Information security management standard |
| **Internal HR Policy** | Company HR Policy Handbook | Defines roles and procedures for internal data use |

**3. Personally Identifiable Information (PII) Collected by MoHRIS**

| **Data Type** | **Source** | **Risk Level** | **Protection Measures** |
| --- | --- | --- | --- |
| Full Name, ID, Contact Info | Employee self-entry | High | Encrypted storage, 2FA |
| Biometric Data (Face/Fingerprint) | Mobile App Scanner | Very High | AES-256 encryption, secure API transmission |
| Employment Contracts | HR uploads | High | Access control, versioning |
| Leave & Attendance Logs | Mobile punch-in/out | Medium | Daily backups, audit logs |
| Salary & Tax Records | Payroll integration | High | Role-based access, masked data display |

**4. Data Lifecycle & Compliance Controls**

| **Stage** | **Control** | **Compliance Tool** |
| --- | --- | --- |
| **Collection** | Consent-based input, privacy notice | In-app consent form, GDPR-style popup |
| **Storage** | Encrypted DBs, regional server hosting | Azure/AWS data region locking |
| **Access** | RBAC (Role-Based Access Control), audit trails | Admin dashboards, login audits |
| **Sharing** | Inter-departmental policies, NDAs | API access tokens, signed data use agreements |
| **Retention** | Legal minimum + internal policy | 7-year retention, automatic purging scripts |
| **Deletion** | User rights for erasure | Admin interface for deletion requests |

**5. Privacy Impact Assessment (PIA)**

| **Risk** | **Likelihood** | **Impact** | **Mitigation** |
| --- | --- | --- | --- |
| Unauthorized biometric data access | Medium | Severe | Encrypted biometric DB, access logging |
| Insider misuse of employee data | High | High | RBAC, separation of duties, background checks |
| Data breach of cloud HR records | Low | Critical | 24/7 monitoring, SSL/TLS protocols, incident response plan |
| Failure to inform employees about data use | Medium | Moderate | Multi-language privacy notices and pop-ups |
| Lack of consent documentation | Medium | Moderate | Digital signature capture with timestamping |

**6. Compliance Activities Timeline**

| **Activity** | **Owner** | **Deadline** | **Status** |
| --- | --- | --- | --- |
| Appoint Data Protection Officer (DPO) | HR Director | Done | ✅ |
| Conduct Data Mapping & Inventory | IT Security Lead | Week 2 | ✅ |
| Draft & Publish Privacy Notice | Legal & Comms Team | Week 3 | ✅ |
| Conduct PIA Review & Sign-Off | DPO | Week 4 | ✅ |
| Internal Audit (Compliance & InfoSec) | Internal Audit | Week 5 | Planned |
| Employee Consent Collection | Project Team | Go-live -1 week | Scheduled |
| External Penetration Test & Report | Cybersecurity Vendor | Go-live -2 weeks | Scheduled |

**7. Documentation Archive**

* Data Protection Impact Assessment (DPIA) Report
* Consent Form Templates (Digital & Paper-based)
* Employee Data Handling SOP
* Data Sharing Agreements
* Internal IT Security Policy
* External Audit Reports
* MoHRIS Compliance Sign-Off Certificate

**8. Continuous Monitoring & Governance**

* Quarterly Privacy Compliance Reviews by DPO
* Annual Security Audits (ISO/IEC 27001 aligned)
* Anonymous Employee Data Privacy Satisfaction Survey
* Real-time Alerts for Data Access Anomalies
* Scheduled Deletion & Retention Compliance Reports

**9. Success Metrics**

| **Indicator** | **Target** |
| --- | --- |
| % of Staff Giving Explicit Consent | ≥98% |
| Security Audit Score | ≥90% Compliance |
| Data Breaches Reported | 0 |
| Data Subject Access Requests Fulfilled on Time | 100% within 21 days |
| Staff Privacy Awareness (Survey) | ≥85% pass score |