**Compliance & Security Requirements Specification**

**Title:** *Comprehensive Compliance & Security Specification for 5G Network Deployment*

**A. Purpose**

Ensure the Smart 5G deployment meets all applicable international standards (GDPR, 3GPP) and local regulatory policies (Kenya Data Protection Act, CAK directives) to protect user privacy, data security, and network integrity.

**B. Compliance Requirements**

| **Area** | **Requirement** | **Reference Standard** | **Implementation Notes** |
| --- | --- | --- | --- |
| **Data Protection** | Personal data must be collected lawfully, with user consent and data minimization applied | GDPR Article 5, Kenya Data Protection Act | Implement user consent management and data anonymization |
| **Data Subject Rights** | Rights to access, rectification, erasure, and data portability | GDPR Articles 15-22 | Provide user portals and processes for exercising rights |
| **Cross-border Data Transfer** | Data must be transferred only to approved jurisdictions with safeguards | GDPR Chapter V, CAK policies | Use Standard Contractual Clauses (SCCs) and encryption |
| **Network Security** | Protect against unauthorized access, data breaches, and network attacks | 3GPP TS 33.501 (5G Security), NIST Cybersecurity Framework | Implement multi-factor authentication, encryption, SEPP |
| **Lawful Interception** | Enable lawful interception with audit trails while preserving user privacy | CAK Telco Regulations, 3GPP TS 33.107 | Integrate LIMS modules with strict access controls |
| **Incident Reporting** | Report breaches within mandated timelines | GDPR Article 33, local laws | Establish SOC and automated breach detection & reporting |
| **User Authentication** | Strong identity verification for subscribers and network entities | 3GPP TS 33.102, SIM Authentication | Implement 5G AKA, SUPI encryption, eSIM provisioning |
| **Network Slice Isolation** | Ensure strict resource and data isolation among network slices | 3GPP TS 28.530 | Deploy slice isolation at data and control planes |

**C. Security Controls**

| **Control Category** | **Specification** | **Compliance Mapping** |
| --- | --- | --- |
| **Encryption** | End-to-end encryption of user plane and control plane traffic | 3GPP TS 33.401, GDPR |
| **Access Control** | Role-Based Access Control (RBAC) with Zero Trust principles | NIST SP 800-207, CAK Policies |
| **Audit & Logging** | Immutable logs of access, configuration changes, and network events | GDPR Article 30, 3GPP TS 33.210 |
| **Vulnerability Management** | Continuous scanning and patch management | OWASP Mobile Top 10, CAK |
| **Physical Security** | Data center security controls and tamper detection | ISO 27001 Physical Controls |
| **AI/ML Security** | Safeguards against adversarial attacks and data poisoning | Emerging best practices |

**D. Compliance Validation Plan**

* Regular audits against GDPR and 3GPP checklist by internal/external teams
* Penetration testing and red-teaming exercises
* Automated compliance dashboards with real-time alerts
* Training & awareness programs for all project staff