Somalia Data Protection Authority (DPA)

Official Codes of Practice & Sector Guidelines

Status: Advisory / Non-Binding Guidance
Version: 1.0
Date of Issue: 2025

The Somalia Data Protection Authority (DPA) issues non-binding Codes of Practice and Sector Guidelines to support organizations in implementing the Somalia Data Protection Act (Law No. 005/2023). These documents provide practical, sector-specific guidance to help entities comply with legal obligations and adopt appropriate safeguards when processing personal data.

Codes of Practice do not create new legal obligations beyond those established in the Somalia Data Protection Act and applicable regulations. However, adherence to these Codes may be taken into account by the DPA when assessing compliance.

Legal Basis

These Codes of Practice and Sector Guidelines are issued pursuant to the supervisory and advisory functions of the Somalia Data Protection Authority under the Somalia Data Protection Act No. 005 (2023).

They are intended to assist organizations in understanding and implementing their statutory obligations under the Act.

Organizations must apply the following expectations proportionate to the nature, scale, and sensitivity of their processing activities.

1. Telecommunications Sector

Telecommunications operators process high volumes of personal and metadata. DPA expects the telecom sector to adopt the following minimum good-practice measures:

1.1 Data Protection Expectations

- Protect subscriber records, SIM registration data, and call detail records (CDRs).
- Apply strong encryption to traffic, signaling, subscriber, and billing information.
- Implement strict access-control mechanisms (least privilege).
- Establish monitoring systems to detect unauthorized access attempts.
- Ensure secure mobile money and airtime transaction processing.
- Ensure that any government or law enforcement access to subscriber data complies with applicable legal procedures and safeguards.

1.2 Additional Safeguards

- Minimize retention of metadata unless justified by legal requirements.
- Subject location-tracking services to heightened risk assessment.
- Apply DPIAs for new digital or mobile-based services.

2. Financial Services Sector (Banking, Fintech, Mobile Money)

Financial institutions process sensitive financial, KYC, and transactional data. DPA recommends:

2.1 Data Protection Expectations

- Implement robust KYC/AML data protection safeguards.
- Encrypt all payment, transaction, and account-related information.
- Enforce multi-factor authentication for customer access.
- Deploy real-time fraud monitoring tools.

2.2 Additional Safeguards

- Require DPIAs for new digital financial services or high-risk products.
- Maintain 24/7 incident detection and reporting capability.
- Conduct documented due diligence and ongoing monitoring of third-party processors and technology providers.

3. Public Sector & E-Government

Government institutions must model strong data protection practices:

3.1 Data Protection Expectations

- Apply strict purpose limitation for all personal data collected.
- Protect digital ID, civil registry, and population-level datasets.
- Ensure secure interoperability without excessive data sharing.
- Adopt transparent, accountable public-sector processing practices.
- Maintain publicly accessible privacy notices explaining government data processing activities where appropriate.

3.2 Additional Safeguards

- Conduct DPIAs for national systems such as ID, immigration, tax, and social services.
- Use strong authentication for staff accessing citizen data.

4. Health Sector

Health data is categorized as highly sensitive.

4.1 Data Protection Expectations

- Protect medical, laboratory, diagnostic, and hospital information.
- Secure electronic health systems and medical record databases.
- Limit access to clinical information to authorized personnel only.
- Ensure healthcare staff are subject to professional confidentiality obligations and periodic security training.

4.2 Additional Safeguards

- Apply encryption and access logging for all patient data systems.
- Require DPIAs for telemedicine, biometric systems, or genomic data processing.

5. Education Sector

Schools and universities handle identifiable information about children and young adults.

5.1 Data Protection Expectations

- Protect student personal records and academic data.
- Secure online learning platforms, portals, and virtual classroom systems.
- Ensure parental consent where legally required.

5.2 Additional Safeguards

- Limit children's data collection to what is strictly necessary.
- Apply DPIAs for digital education tools and surveillance systems.
- Ensure digital education systems apply privacy-by-design and privacy-by-default principles.

6. Humanitarian and NGO Sector

Humanitarian actors often process vulnerable-population data.

6.1 Data Protection Expectations

- Protect beneficiary registration, displacement, biometrics, and vulnerability data.
- Ensure lawful bases for data collection in crisis contexts.
- Apply strict access controls and secure humanitarian data-sharing channels.

6.2 Additional Safeguards

- Conduct DPIAs for large-scale or biometric registration activities.
- Ensure cross-border humanitarian data transfers comply with the Act's transfer mechanisms and safeguards.

7. Security & Surveillance Services

Surveillance data creates high privacy risks.

7.1 Data Protection Expectations

- Process surveillance data in accordance with legality, necessity, and proportionality principles.
- Minimize retention of CCTV recordings and biometric logs.
- Apply robust controls on devices and monitoring systems.

7.2 Additional Safeguards

- DPIAs are required before deployment of new surveillance technologies.
- Certain high-risk surveillance deployments may require prior authorization where provided for under the Act or applicable regulations.

Review and Updates

The DPA may review and update these Codes of Practice periodically to reflect technological developments, emerging risks, and regulatory priorities.

Need Additional Guidance?

DPA is continuously developing sector-specific Codes of Practice, templates, and advisory notes.

Organizations may contact DPA for clarification, consultation, or tailored guidance.

Disclaimer

These Codes of Practice and Sector Guidelines are issued to provide practical assistance in applying the Somalia Data Protection Act No. 005 (2023).

They do not replace statutory provisions and do not create additional legal obligations. Organizations remain responsible for ensuring full compliance with applicable law.