DATA PROTECTION AUTHORITY

SOMALIA

GUIDANCE NOTE ON REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

2024

DPA

SOMALIA

GUIDANCE NOTE ON REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

SOMALIA

Introduction

This guidance note outlines the requirements for registration as a Data Controller or Data Processor, as mandated by the Act, and provides detailed guidance on compliance and best practices. It is designed to assist entities in understanding their obligations under the Somalia Data Protection Act.

Definitions

Act: Somalia Data Protection Act.
Data Controller: An entity that determines the purpose and means of processing personal data.
Data Processor: An entity that processes personal data on behalf of the Data Controller.
Data Subject: An individual whose personal data is being processed.
Entity: Any natural or legal person, public authority, agency, or other body that processes personal data.
Processing: Any operation performed on personal data, whether by automated means or otherwise, such as collection, storage, and dissemination.
Sensitive Personal Data: Data revealing racial or ethnic origin, political opinions, religious beliefs, or health information, among others.

DPA

SOMALIA

Scope and Purpose

This guidance note aims to clarify the registration process and the obligations of Data Controllers and Data Processors. The Somalia Data Protection Act requires all entities processing personal data to register with the Data Protection Authority (DPA) of Somalia, subject to thresholds set by the DPA.

Types of Entities

The Act categorizes entities into Data Controllers and Data Processors. Entities may register as both, provided they fulfill the criteria for each category.

Data Controllers

A Data Controller is responsible for determining the purpose and means of processing personal data. They must ensure compliance with all data protection principles and are accountable for the actions of any Data Processors they engage.

You are Data Controller if you:

- ✓ Decide to collect or process personal data.
- ✓ Determine the purpose and means of processing.
- ✓ Decide which personal data to collect and from whom.
- ✓ Gain commercial or other benefits from processing.
- ✓ Process data as part of a contract with the data subject.
- ✓ Employ data subjects whose data is processed.
- ✓ Make decisions about individuals as part of processing.
- ✓ Exercise professional judgment in processing personal data.
- ✓ Have a direct relationship with data subjects.
- ✓ Autonomously decide how data is processed.
- ✓ Appoint processors to handle data on their behalf.

Data Processors

A Data Processor processes personal data on behalf of a Data Controller, without deciding the purpose or means of processing.

You are Data Processors if you:

- ✓ Handle personal data based on a contract with a Data Controller.
- ✓ Follow instructions from the Data Controller.
- ✓ Do not decide on the collection, purpose, or disclosure of personal data.
- ✓ May make decisions on how data is processed under a contract.
- ✓ Do not consider Data Processors if they are employees of the entity.

Registration Requirements

Entities must register as either *Data Controllers or Data Processors* unless they qualify for exemptions. The registration process involves providing detailed information about data processing activities and ensuring compliance with data protection principles.

Information Required for Registration:

- Name and address of the entity.
- Contact details of the Data Protection Officer.
- Description of personal data processed.
- Categories and number of data subjects.
- Purposes of data processing.
- Categories of recipients of personal data.
- Details of international data transfers.
- Description of risks, safeguards, and security measures.
- Any additional information required by the DPA.

Fees and Levies

The DPA may prescribe annual fees or levies for registered entities to cover administrative costs. Fees may vary based on the size and class of the entity, with exemptions for government bodies.

Fee Structure

S/N	Entity Category	Reg. Fee
1.	Micro-entities: [Less than 5 Employees]	Exempt.
2.	Small entities: [5 – 50 Employees]	$xx
3.	Medium entities: [51 – 99 Employees]	$xx
4.	Large entities: [More than 99 Employees]	$xx
5.	Government bodies:	Exempt.
6.	Non-profits Organizations.	$xx

Designation of Data Protection Officers (DPO)

Entities must designate a Data Protection Officer (DPO) with expertise in data protection laws and practices. The DPO's responsibilities include advising the entity on compliance, monitoring data protection practices, and acting as the contact point for the DPA.

DPO Responsibilities:

- Inform and advise the entity and employees about their obligations.
- Monitor compliance with the Act and other data protection laws.
- Provide advice on data protection impact assessments.
- Cooperate with the DPA.
- Act as the contact point for the DPA on issues relating to processing.

Processing of Applications

1. **Submission:** Applications must be submitted in the prescribed form along with the required documentation and fees.
2. **Verification:** The DPA will verify the details provided in the application.
3. **Approval:** If the application meets the requirements, the DPA will issue a certificate of registration.
4. **Renewal:** Registrations must be renewed every 12 Months. Renewal applications should be submitted before the expiry of the current registration.

Data Protection Principles

Entities must adhere to the following principles:

A. **Lawfulness, Fairness, and Transparency:** Data processing must be lawful, fair, and transparent to data subjects.
B. **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
C. **Data Minimization:** Data collected must be adequate, relevant, and limited to what is necessary.
D. **Accuracy:** Data must be accurate and, where necessary, kept up to date.
E. **Storage Limitation:** Data must be kept in a form that permits identification of data subjects for no longer than necessary.
F. **Integrity and Confidentiality:** Data must be processed in a manner that ensures appropriate security.
G. **Accountability:** The Data Controller is responsible for, and must be able to demonstrate, compliance with these principles.

Enforcement and Compliance

The DPA has the authority to enforce compliance with the Act. This includes addressing complaints from data subjects, conducting audits, and initiating investigations. Non-compliant entities may face enforcement actions, including fines and penalties.

Penalties for Non-Compliance:

- Administrative fines up to $xx for minor infringements.
- Higher fines up to $xx for serious infringements.
- Orders to cease processing activities.
- Suspension or revocation of registration.

Conclusion

Entities processing personal data in Somalia must understand and fulfill their obligations under the **Somalia Data Protection Act**. This includes registering with the DPA, ensuring compliance with data protection principles, and appointing a qualified DPO. This guidance note serves as a comprehensive resource for understanding these requirements and ensuring compliance