DPA Guidance

1. introduction

In Somalia, data protection is founded on the constitutional rights, basic personal liberties and limitations under article 13 of the Constitution of the Federal Republic of Somalia 2012 ('the Constitution'). The Somali Data Protection Act 2023 ('DPA') is Somalia's main data protection legislation. The DPA was enacted on March 23, 2023, and has been in effect since then.

Prior to the DPA, the Somali Data Protection Act, 2023. Although enforceable, it remains a subsidiary legislation, and there was no specific commission to oversee data protection.To temporarily assist with supervision, the Somali Government ('the Government') issued an executive order in February 2023 that established the Somali Data Protection Authority and transferred the data protection role as well as the existing regulations or guidance issued by DPA. DPA was created to oversee data protection in Somalia.

1.1. Key acts, regulations, directives, bills

The following laws and regulations contain provisions for data protection:

- The Somali Federeal Constitution;
- Data Protection Law Act
- General Data Protection Regulations, EU.

2. Scope of Application

2.1. Personal scope

The main legislation on data protection in Somalia is the DPA, The DPA applies to the processing of personal data whether or not by automated means (Article 14 of the DPA).

2.2. Territorial scope

The DPA applies where:

- data controller or data processor is domiciled in, resident in, or operating in Somalia;
- processing of personal data occurs within Somalia; or
- the data controller or the data processor is not domiciled in, resident in, or operating in Somalia, but is processes personal data of a data subject in Somalia.

The Data Protection Law Act applies to Somali citizens regardless of where they reside. The DPA will apply to a data controller so long as the data of a Somali citizen is collected. The DPA will have extra-territorial scope in its application.

2.3. Material scope

The Data Protection Act applies to any data controller that processes the personal data of anyone residing in Somalia or to Somalia within the country.

The DPA does not apply to the processing of personal data for personal or household purposes. The DPA also does not apply to the processing of personal data:

- carried out by a competent authority to prevent, investigate, detect, prosecute, or adjudicate any criminal offense or execution of criminal penalty;
- carried out by a competent for national security purposes;
- carried out by a competent authority to prevent or control a national public health emergency; or
- for public interest publication, defense of legal claims whether in court or administrative or out-of-court proceedings.

3. Data Protection Authority | Regulatory Authority

3.1. Main regulator for data protection

The Data Protection Authority is the main supervisory and regulatory authority for data protection in Somalia. The DPA oversees the implementation of the Data Protection Act and matters relating to data protection in Somalia (Article 6 and 7 of the DPA).

3.2. Main powers, duties and responsibilities

The Data Protection Authority has the power to issue regulations, investigate alleged violations of the Data Protection Act, and impose fines data for contravention of the Act (Article 7 of the DPA). The data Protection Authority has the responsibility to register data controllers and data processors of major importance; promote awareness regarding the obligations of data controllers and data processors; accredit, license, and register data protection compliance service; receive complaints about violations of the personal Data; and advise the government on data protection.

4. Key Definitions

Personal data: means any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.

Sensitive data: means personal data related to an individual's:

- genetic and biometric data, for the purpose of uniquely identifying a natural person;
- race or ethnic origin;
- health status;
- political opinions or affiliations;
- trade union memberships; or

- any other personal data prescribed by the DPA as sensitive personal data pursuant to Article 2(15) of the DPA.

Data controller: means an individual, private entity, public commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing personal data.

Data controller or data processor of major importance: means a data controller or data processor that is domiciled, resident in, or operating in Somalia and processes or intends to process personal data of more than such number of data subjects who are within Somalia, as the Data Protection Authority may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Somalia as the Data Protection Authority may designate.

Data processor: means an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor.

Data subject: means an individual to whom personal data relates.

Biometric data: means any personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of an individual, which allows or confirms the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition, and deoxyribonucleic acid (DNA) analysis.

Pseudonymization: means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Consent: means any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or affirmative action, of an

individual's agreement to the processing of personal data relating to them or to another individual on whose behalf they have the permission to provide such consent.

Automated decision-making: means a decision based solely on automated processing by automated means, without any human involvement.

5. Legal Bases

5.1. Consent

Article 17 of the Data Protection Act stipulates that processing shall be lawful where the data subject has given consent to the processing of personal data for one or more specific purposes. The data controller must also demonstrate that the data subject has the legal capacity to consent.

An individual has the right to withdraw consent and a data controller has an obligation to make it easy for an individual to withdraw just as it is easy to give consent. (Article 21 of the DPA).

5.2. Contract with the data subject

Article 14 of the DPA provides that the processing of personal data is lawful where the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering a contract.

5.3. Legal obligations and Interests of the data subject

Processing of personal data is lawful where the processing of the data is necessary for compliance with a legal obligation to which the data controller or data processor is subject, and also processing personal data is necessary to protect the vital interest of the data subject or of another natural person (Article 14 of the DPA)

5.4. Public interest

Processing of personal data is also lawful where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor (Article 14 of the DPA)

6. Principles

Transparency

Where a data controller is processing personal information, the data subject has to be informed without constraint or unreasonable delay (Article 19 of the DPA). A data controller has an obligation to take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, and for any information relating to a child (Article 16 of the DPA). In addition, prior to collecting personal data from a data subject, a data controller has to inform the data subject of the purpose(s) of the processing for which the personal data is intended as well as the legal basis for the processing.

Purpose and limitation

A data controller has an obligation to specify the purpose of processing personal data (Article 14 of the DPA). Where a data controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the controller shall provide the data subject prior to that further processing with information on that other purpose, and with any relevant further information.

Limitation and Accuracy

The provisions of the DPA are sacrosanct and no limitation clause in a privacy policy will exonerate a data controller from liability for violating the DPA Personal data is expected to be accurate and without prejudice to the dignity of

the human person. A data subject has the right to access and rectify their data (Article 15 of the DPA).

Storage Limitation

A data controller should stipulate the period of storage or if not possible, the criteria used to determine that period (Article 15 of the DPA). A data controller should stipulate in its privacy policy the period for which personal data will be stored, or if that is not possible, the criteria used to determine that period.

Confidentiality

A data controller is required to put in place a data security apparatus to keep the collected data confidential and protect it against attacks (Article 24 of the DPA).

Accountability

Anyone who is entrusted with the personal data of a data subject or who is in possession of such data is accountable for its acts and omissions in respect of data processing and in accordance with the principles contained in the DPA.

7. Controller and Processor Obligations

Obligations of the data controller or data processor under the DPA include:

- ensuring that where a data processor is engaged, the data processor complies with the DPA when processing personal data.
- a data controller assisting the data processor by use of appropriate technical and organizational measures to ensure the rights of a data subject are honored (Article 32 of the DPA).
- implement appropriate technical measures to ensure the security, integrity, and confidentiality of personal data.
- provide the data controller or data processor with the information required to ensure compliance (Article 2 of the DPA); and
- notify the existing data processor where a new data processor is engaged.

Under the DPA, Data controller must:

- designate a data protection officer ('DPO') for the purpose of ensuring adherence to the Data Protection Regulations, relevant data privacy instruments, and data protection directives of the data controller - the data controller may outsource data protection to a verifiably competent firm or person (Article 34);
- ensure continuous capacity building for its DPOs and the generality of its personnel involved in any form of data processing.
- ensure that consent of a data subject has been obtained without fraud, coercion, or undue influence.
- send a soft copy of the summary of the audit containing information about processed data to where it processes the personal data.

7.1. Data processing notification

Where a data controller processes the personal data of more than 1000 data subjects in a period of six months, a soft copy of the summary of a required audit must be submitted to the DPA, stating its privacy and data protection practices including:

- personally identifiable information the organization collects on employees of the organization and members of the public;
- any purpose for which the personally identifiable information is collected;
- any notice given to individuals regarding the collection and use of personal information relating to that individual;
- any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
- whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
- the policies and practices of the organization for the security of personally identifiable information;
- the policies and practices of the organization for the proper use of personally identifiable information;
- organization policies and procedures for privacy and data protection;
- the policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies; and
- the policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies (Article 24 od the DPA).

Data controllers who process the personal data of more than 200 data subjects in a period of 12 months are required to submit a summary of its data protection

audit to the DPA, the data protection audit must contain information as specified above.

- the contact details of the data protection officer;
- the purpose(s) of the processing for which the personal data is intended as well as the legal basis for the processing;
- the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the DPA;
- period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a relevant authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject with the basis for this further processing; and
- where applicable, that the controller intends to transfer personal data to a recipient in a foreign country or international organization and the existence or absence of an adequacy decision by the DPA.

The DPA registers and licenses DPOs who monitor, audit, conduct training, and data protection compliance consulting to all data controllers on its behalf (Article 34 of the DPA). Audits submitted pursuant and must be accompanied by a verification statement by a licensed DPO. Each controller is expected to pay the following filing fees for annual audit.

7.2. Data transfers

A data controller is allowed to transfer personal from Somalia to another country as long as there is an adequate level of protection of personal data in such country (Article 31 of the DPA) or the data subject consented to the transfer after being informed of the risk and did not withdraw the consent, the transfer is necessary for the performance of a contract to which the data subject is a party, the transfer is for the data subject's benefit, necessary for a public interest, necessary for legal action, or protect the vital interest of the data subject or third party.

In determining the adequacy of a third country or organization, the following considerations will be born in mind:

- the legal system of the foreign country notably as it relates to human rights protection, the rule of law, and relevant legislation;
- implementation of such legislation;
- the existence and effectiveness of an independent supervisory authority in the foreign country or whether an international organization is responsible for compliance with data protection, assisting and advising the data subjects in exercising their rights and cooperation with the relevant authorities in Somalia; and
- the commitments of the foreign country or international organization to data protection through conventions, instruments, and participation in multilateral or regional systems.

Under Articles 17 and 18 of the DPA, the exceptions to the above requirements are:

- where the data subject has given their consent after being informed of the risk;
- where the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- where the transfer is necessary for important reasons of public interest;
- where the transfer is necessary for the establishment, exercise, or defense of legal claims; and

- where the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

The data subject should be aware of possible violations of their rights in the foreign country.

7.3. Data processing records

There is an obligation to maintain data processing records. Article 19 of the DPA requires data controllers to conduct a detailed audit of their privacy and data protection practices with at least each audit stating:

- personally identifiable information the organization collects on employees of the organization and members of the public;
- any purpose for which the personally identifiable information is collected;
- any notice given to individuals regarding the collection and use of personal information relating to that individual;
- any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
- whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
- the policies and practices of the organization for the security of personally identifiable information;
- the policies and practices of the organization for the proper use of personally identifiable information;
- organizational policies and procedures for privacy and data protection;
- the policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies; and
- the policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

7.4. Data protection impact assessment

A data controller is required to conduct a privacy impact assessment where the processing of personal data may likely result in high risks to the rights of a data subject (Article 29 of the DPA). The data controller will have to consult the DPO prior to processing where the impact assessment indicates that the processing would result in a high risk to the rights and freedom of a data subject (Article 18 DPA).

The DPA Implementation Framework

The Implementation Framework requires that data controllers and processors conduct a Data Protection Impact Assessment ('DPIA') in accordance with the provisions of the DPA (Article29).

the Implementation Framework states that data controllers and processors/administrators must conduct DPIAs as part of enhancing compliance and reducing liabilities, within their compliance checklist, where applicable.

Where the organization intends to embark on a project that would involve the intense use of personal data, a DPIA should be conducted to identify possible areas where breaches may occur and devise a means of addressing such risks. Organizations are expected to conduct a DPIA on their processes, services, and technology periodically to ensure continuous compliance).

Furthermore, DPA may request the submission of a DPIA from any data controller or processor/administrator where such processing activities are deemed to be of high impact on data subjects. A DPIA may be required for the following types of processing,

- evaluation or scoring (profiling);
- automated decision-making with legal or similar significant effects;
- systematic monitoring;
- when sensitive or highly personal data is involved;
- when personal data processing relates to vulnerable or differently-abled data subjects; and
- when considering the deployment of innovative processes or the application of new technological or organizational solutions.

7.5. Data protection officer appointment

Under DPA, a data controller of a major importance is required to have a Data Protection Officer (DPO). The DPO may be an employee, or someone engaged to provide such service (Article 34 of the DPA). The DPO will advise data controllers or data processors regarding the processing of personal data, monitor compliance with the DPA and act as contact point for the DPA on issues relating to data processing.

Meanwhile, under the DPA, both data controller and processor are required to appoint a DPO. A data controller or processor can also outsource to a verifiably competent firm or person. There are no specific requirements in this regard. A data controller or processor has to ensure continuous capacity building for its DPO, and its personnel involved in any form of data processing.

The Implementation Framework specifies that a data controller is required to appoint a dedicated DPO within six months of commencing business or within six months of the issuance of the Implementation Framework itself, where one or more of the following conditions are present.

- the entity is a government organ, ministry, department, institution or agency;
- the core activities of the organization involve the processing of personal data of more than 1,000 data subjects annually;
- the organization processes sensitive personal data in the regular course of its business; and
- The Data Protection Authority has a provision for the role of the Data Pprotection Officer, A DPO must have verifiable professional expertise and knowledge of data protection to do the following,

- inform and advise the business, management, employees, and third parties who carry out processing, of their obligations under the DPA;
- monitor compliance with the DPA and with the organization's own data protection objectives;
- assignment of responsibilities, awareness-raising, and training of staff involved in processing operations;
- provide advice where requested as regards a Data protection impact assessment and monitor its performance;

7.6. Data breach notification

A personal data breach refers to an event that results in transferred, stored or otherwise processed personal data is accidentally or unlawfully destroyed, lost or changed. Unauthorized disclosure of data and unauthorized access are also considered a breach of data security to information. Data breach can create huge legal, financial and reputational upsets that could damage an organization and must be avoided.

7.7. Data retention

For each category of personal data, your organization must list the period for which the data is intended to be kept.

It is important to note that there is a general rule in which data must not be retained for longer than is necessary, considering the purpose of why it was collected.

7.8. Children's data

There are specific provisions that regulate the processing of a child's data.

A data controller has an obligation to obtain consent from a data subject's parent or legal guardian if the data subject is a child (Article 16 of the DPA). However, consent may not be required, where the processing is to protect the vital interest of a child, the processing is for educational, medical, or social care and done under the supervision of a professional, or necessary for court proceedings.

7.9. Special categories of personal data

A data controller or data processor is prohibited from processing sensitive personal data. However, there are exceptions to this rule, including,

- where a data subject consents and has not withdrawn consent for the purpose of processing;
- processing is necessary to for performing the data controller's obligation or exercise of a data subject's rights;
- processing is necessary to protect the vital interests of a data subject or another person;
- processing is carried out in the course of a data controller's legitimate activities;
- processing is necessary for legal proceedings;
- processing necessary by reason of substantial public interest;
- for medical care or community welfare; and
- for public health or research purposes.

7.10. Controller and processor contracts

Article 19 of the DPA provides that a data controller and processor have a duty to take reasonable measures to ensure that a party to a data processing contract (other than the data subject) does not have a record of violating the rights of a

data subject. Moreover, every data controller and processor shall be liable for the actions or inactions of third parties that handle the personal data of data subjects under the DPA.

8. Data Subject Rights

Under Article 20 of the DPA, data subjects have the following rights:

- right to be informed of the processing of data;
- right to complain or send a request to the data controller;
- right to obtain information about their data from the data controller free of charge except as otherwise provided by regulation or public policy;
- right to know the details of the data controller;
- right to withdraw consent;
- right to access their personal data;
- right to data portability;
- right to data rectification;
- right to restrict or object to the processing of their data;
- right to be informed where their data is being processed for additional purposes;
- right to be informed about the transfer of their data to another country;
- right to complain to the relevant authority; and
- right to data deletion.

8.1. Right to be informed

A data controller is required to take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and for any information relating to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means (Article 18 of the DPA).

8.2. Right to access, rectification and erasure

A data subject has the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used, and machine-readable format, and have the right to transmit that data to another data controller without hindrance from the data controller to which the personal data

has been provided. A data subject has the right to have an access, be notified and to be erasure by the data controller of the rectification of data (Article 20 of the DPA).

8.3. Right to object/opt-out

Data subjects have the right to withdraw their consent to the processing of their personal data at any time. In addition, a data subject may choose to object to the processing of personal data relating to them which the data controller intends to process for the purpose of marketing (Article 22 of the DPA).

8.4. Right to data portability

A data subject has the right to transmit personal data from one data controller to another without hindrance from the data controller (Article 30 of the DPA).

8.5. Right not to be subject to automated decision-making

Prior to collecting personal data from a data subject, the data controller has to provide the data subject with information regarding the existence of automated decision-making (Article 23 of the DPA).

9. Penalties

The DPA has wide powers under Article 33 of the DPA where a data controller violates the same irrespective of criminal sanctions including:

- requiring the data controller or data processor to remedy the violation;
- ordering the data controller or data processor to pay compensation to the data subject for the injury, loss, or harm suffered;
- ordering the data controller or data processor to account for profits earned from the violation;
- ordering the data controller or data processor to pay a penalty or remedial fee.

The penalty or remedial fee may be an amount up to the higher maximum amount, in the case of a data controller or data processor of major importance; or the standard maximum amount in the case of a data controller or data processor not of major importance.

10. Online Privacy

Data Protection Authority Somalia requires all mediums through which Personal Data is collected or processed to display a simple and conspicuous privacy policy, easily understood by the targeted Data Subject class. A violation of personal rights may be subject to civil enforcement. The privacy policy must contain the following, in addition to any other relevant information:

- What constitutes Data Subject consent;
- Description of Personal Data to be collected;
- Purpose of Personal Data collection;
- Technical methods used to collect and store personal information (i.e. cookies, web tokens, etc.);
- Access (if any) of third parties to Personal Data and purpose of access;
- An overview of data processing principles under the DPA;
- Available remedies for privacy policy violations;
- Timeframes associated with available remedies; and
- Any limitation clause, provided that no limitation clause shall avail any Data Controller who acts in breach of the principles of lawful processing set out in the Data Protection Authority.