LAW NO. [005] OF [2023]
DATA PROTECTION ACT

ARRANGEMENT OF ARTICLES

CHAPTER I—PRELIMINARY

CHAPTER II—ADMINISTRATION

CHAPTER III—PRINCIPLES GOVERNING PROCESSING OF PERSONAL DATA

CHAPTER I—PRELIMINARY PROVISIONS

Article 1: Name of the Law

This Law shall be cited as the "Data Protection Act."

Article 2: Definitions

In this Law, unless the context otherwise requires, the following words shall have their respective meaning as below:

1. "**Authority**" means the Data Protection Authority, as established in article 6;
2. "**Binding corporate rules**" means personal data protection policies and procedures adhered to by the members of a group of firms under common control with respect to the transfer of personal data among such members;
3. "**Biometric data**" means personal data resulting from specific technical processing relating to an individual's body or behaviour, which allow or confirm 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;
4. "**Certification mechanism**" means a process by which the Authority or a third-party entity registered by the Authority confirms that personal data protection policies and procedures of data controllers or data processors comply with specified standards;
5. "**Child**" means an individual below eighteen years of age;
6. "**Consent**" means any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement;
7. "**Data controller**" means an individual, private entity, public authority or agency or any other body who or which, alone or together with others, determines the purposes and means of the processing of personal data;
8. "**Data controller of major importance**" means a data controller that is domiciled, resident or operating in the Federal Republic of Somalia and processes, or engages one or more data processors that collectively process, personal data relating to data subjects who are within the Federal Republic of Somalia;

9. "**Data processor**" means an individual, private entity, public authority or agency or any other body who or which processes personal data on behalf of or at the direction of a data controller or another data processor;
10. "**Data subject**" means an individual to whom personal data relates;
11. "**Minister**" means the Minister of Communications and Technology or such other Minister designated as responsible for data protection;
12. "**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;
13. "**Personal data breach**" means a breach of security of a data controller or data processor leading to or reasonably likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
14. "**Data processing**" means the collection, recording, organisation, storage, alteration, disclosure by transmission, combination, restriction or destruction of personal data by electronic means; and
15. "**Sensitive personal data**" means personal data relating to an individual's:
    a) biometric data;
    b) race, clan or ethnic origin;
    c) religious beliefs;
    d) health status;
    e) marital status or sex life; or
    f) political opinions or affiliations; and
    g) any other category of personal data prescribed by the Authority in regulations as sensitive personal data.

Article 3: Objectives

The objectives of this Law are to:

1. protect data subjects from risks to data subjects arising from the processing of their personal data, including risks to their rights and liberties under the Constitution of the Federal Republic of Somalia;
2. promote data processing practices that protect the security of personal data and privacy of data subjects;

3. ensure that personal data is processed in a fair, lawful and accountable manner;
4. facilitate the secure transfer of personal data about citizens and residents of the Federal Republic of Somalia held by international organisations to appropriate government entities for purposes of providing public services and related governmental functions;
5. establish a framework for secure government processing of personal data to enhance the welfare of the people of the Federal Republic of Somalia;
6. increase the beneficial use of personal data in the digital economy of the Federal Republic of Somalia and its participation in regional and global economies;
7. establish an authority designated for the protection and oversight of public and personal data within the Federal Republic of Somalia.

Article 4: Scope of the Law

This Law applies only to a data controller where:

1. the data controller is domiciled, resident or operating in the Federal Republic of Somalia;
2. the processing occurs within the Federal Republic of Somalia; or
3. the processing relates to the monitoring of the behaviour of, or targeted offering of goods or services to, a data subject in the Federal Republic of Somalia.

Article 5: Exemptions

1. This Law does not apply to the processing of personal data solely for personal, recreational or household purposes.
2. Subject to sub-article 3, data controllers that are domiciled, resident, or operating in the Federal Republic of Somalia are exempt from this Law:
   a) if they process personal data relating to data subjects who are within the Federal Republic of Somalia; and
   b) until the second anniversary of the date on which it comes into force, if they are not data controllers of major importance.
3. This Law does not apply to processing of personal data:
   a) by competent authorities for the purposes of the prevention, investigation, detection, prosecution or adjudication of criminal offences or the execution of criminal penalties;
   b) by competent authorities for the purposes of prevention or control of a national public health emergency;

c) by competent authorities as necessary for national security; or necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure; so long as such processing uses reasonable, proportionate and effective measures to safeguard the fundamental rights and the interests of the data subject.

4. This Law does not apply to processing carried out for purposes of journalistic, educational, artistic or literary expression to the extent that the obligations and rights in this Law would be incompatible with such purposes.

CHAPTER II— ADMINISTRATION

Article 6: The Data Protection Authority

1. There shall be established the Data Protection Authority, which shall have legal personality and the power to own property, enter into contracts and owe obligations, and to sue and be sued in its name in accordance with procedures for defending or suing government institutions.
2. The Authority shall be constituted as a new independent agency with the functions, powers and duties under this Law upon the:
   a) adoption of this Law by Both Houses of the Federal Parliament and promulgation by the President of the Federal Republic of Somalia; and
   b) appointment of the General Manager who shall be in charge of the Authority.
3. Except as otherwise provided in this Law, the Authority shall be independent in carrying out its duties under this Law and there shall be no interference from the Minister or other government institutions.
4. Notwithstanding sub-article 3, the Authority shall:
   a) have regard to general policy directions and laws given from time to time by the Government provided such directions are consistent with this Law; and
   b) comply with directions from the President and Cabinet in the interests of national security, public order and the defence of the Federal Republic of Somalia.
5. The revenue of the Authority for its activities under this Law shall comprise:
   a) allocations from the general budget of the Government; and
   b) revenues from administrative penalties, fees, levies and fines made under this Law.

6. The Authority shall prepare, publish and submit to the Minister a report relating to the activities of the Authority during the immediately preceding financial year.

Article 7: Mandate, powers and functions of the Authority

1. The Authority shall promote the protection of personal data, oversee the implementation of this Law, and be responsible for its enforcement, throughout the Federal Republic of Somalia.
2. The Authority shall exercise the powers set out in this Law and shall perform the following functions:
   a) promote public awareness of the risks relating to personal data, of personal data protection and the rights granted and obligations imposed under this Law;
   b) encourage the introduction of technological and administrative measures to enhance personal data protection in accordance with recognized international standards and applicable international law;
   c) participate in international fora and engage with other national, regional and international authorities responsible for data protection with a view to developing consistent and efficient approaches to regulation of cross-border transfers of personal data;
   d) oversee the Government institutions as they implement data protection policies as required by this Law or international law;
   e) submit legislative proposals to the Minister, including amending existing laws, with a view to strengthening personal data protection in the Federal Republic of Somalia;
   f) collect and publish information with respect to personal data protection, including personal data breaches;
   g) receive complaints of and investigate violations of this Law or regulations, rules or other subsidiary legislation or orders issued hereunder;
   h) impose administrative penalties in case of violations of this Law or any regulations, rules or other subsidiary legislation or orders made hereunder;
   i) designate countries, regions, sectors, international organisations or measures as affording or not affording adequate personal data protection standards for cross-border transfers;
   j) make sure that the Federal Republic of Somalia complies with its international obligations relating to data protection;

k) render technical assistance on data protection matters to the President, the Prime Minister, and the Cabinet;

l) register and levy fees on data controllers of major importance;

m) submit proposals through the Minister to the Cabinet for regulations to be made under this Law;

n) issue directives and opinions, make recommendations and rules and publish guidance as required to give effect to and further specify the application of this Law; and

o) register data controllers, data processors, data protection officers, and audit entities that audit data controllers and data processors.

3. The Authority may publish guidance on good practices in, and development of, codes of conduct on data protection and compliance with this Law.

Article 8: The Board of the Authority

1. The Authority shall have a Board of up to nine members in accordance with Article 9.
2. As to fully operationalize the Authority, members of the Board shall be appointed when:
    a) The General Manager prepares and completes all things necessary for the establishment and functioning of the Authority;
    b) An appropriation is made for the Authority in the Budget of the Federal Government;
    c) The Authority secures a headquarters for the discharge of its functions.
3. The appointed General Manager shall execute all duties necessary before the appointment of the Board within two years from the time this Law comes into force.

Article 9: Members of The Board

1. The Authority shall have a Board of up to nine members comprising:
    a) one member appointed by the Minister from the Ministry;
    b) one member appointed by the Minister from the private sector of Somalia with not less than five years' experience in matters relating to the digital economy;
    c) one member appointed by the Minister from civil society representing the interests of data subjects with not less than five years' experience in matters relating to data protection or consumer protection;

d) one lawyer appointed by the State Attorney General from the Office of the State Attorney General;

e) the General Manager;

f) up to four other members having not less than five years' experience in matters relating to digital economy, data protection or consumer protection.

2. Membership of the Board shall be a part-time engagement.

3. Members of the Board shall receive compensation for all costs incurred for the meetings held in every three months unless the General Manager calls an extraordinary meeting.

4. The General Manager and members of the Board shall hold office for a term of four years which may be renewed only twice.

5. The members of the Board shall elect a Chairperson of the Board among themselves every four years.

6. The Board's duties are:

a) setting the overall policy and general supervision of the affairs of the Authority toward the efficient and effective discharge of the Authority's functions;

b) approving strategic plans, action plans and budgets submitted by the General Manager;

c) supervising the implementation of this Law and any approved strategic plans or action plans;

d) approving annual reports submitted by the General Manager;

e) approving the Authority's recruitment plan while considering the need for professionals and the limitations of the budget;

f) fixing the terms and conditions of service of the employees of the Authority, including remuneration, allowances and pension benefits;

g) making, altering, or revoking disciplinary rules and procedures and measures for the staff, officers and other employees of the Authority;

h) providing advice and counsel to the General Manager;

i) submitting progress reports about the management plan of the Authority to the Cabinet, as requested.

Article 10: The General Manager and staff of the Authority

1. The General Manager shall:

a) be the highest official in the Authority;

b) be responsible for leadership and the management of the Authority's daily functions and ensuring that the Authority is fulfilling its mandate under this Law; and

c) have the legal power to represent the Authority.

Article 11: Removal of a Board member or General Manager

A member of the Board or the General Manager shall be removed from office if such person:

1. has been adjudged or otherwise declared bankrupt under any law in force in any part of Somalia;
2. is convicted of an offence involving dishonesty, fraud or forgery or any other offence punishable for five years or more by any competent court of law in Somalia;
3. is medically certified by a duly qualified and authorised doctor to be of unsound mind or becomes incapable through illness or injury of performing his or her duties; or
4. is guilty of serious misconduct in relation to his or her duties following an investigation into any matter relating to his or her duties in which he was accorded fair hearing.

Article 12: Conflicts of interest

1. No Board member or General Manager or any staff of the Authority may have an interest in any data controller of major importance or any data controller or data processor that is the subject of any compliance review, investigation, enforcement or any other regulatory proceeding of the Authority.
2. An interest under sub-article 1 includes:
   a) an economic interest of his or her spouse, immediate family members or other relatives;
   b) an economic interest of a company in which he or she holds shares or other securities, directly or indirectly;
   c) an economic interest of his or her business partner;
   d) negotiating or being party to an agreement to act as representative, agent or employee of, or provide any other service to, the data controller or data processor.
3. If a Board member, General Manager or any staff of the Authority has an interest as contemplated in sub-article 1, then he or she shall either:

a) disclose the interest to the Board and recuse himself or herself from any activity relating to the relevant data controller or data processor, and shall receive no information about such matter; or

b) irrevocably and immediately divest the interest to the satisfaction of the Board; or

c) resign from his or her position with the Authority.

CHAPTER III— PRINCIPLES GOVERNING PROCESSING OF PERSONAL DATA

Article 13: Establishment of the Data Protection Authority

1. The Authority is an independent agency in accordance with article 6 and shall become an authority vested with all of the functions, powers and duties provided for in this Law.
2. The Authority shall have a General Manager proposed by the Minister, confirmed by the Cabinet, and appointed by the President of the Federal Republic of Somalia:
    a) the General Manager shall have experience and expertise in matters of data protection, government administration, business or law;
    b) the General Manager shall be responsible for carrying out the functions, exercising the powers and performing the duties of the Authority under this Law;
    c) the activities of the Authority shall be funded from allocations from the National Budget and revenues from administrative penalties, fees, levies and fines made under this Law.
3. the Minister shall ensure that the General Manager has the staff and resources required to carry out the functions of the Authority under this Law.

Article 14: Lawfulness of processing of personal data

1. A data controller shall ensure that personal data is processed fairly, in a transparent manner and in accordance with sub-article 2.
2. A data controller shall not process personal data, or permit personal data for which it is responsible to be processed, unless:
    a) the data subject has given and not withdrawn consent for the specific purpose or purposes for which it will be processed;
    b) the processing is necessary for the entering into or performance of a contract with the data subject;

c) the processing is necessary for compliance with a legal obligation;

d) the processing is necessary for the establishment, exercise or defence of a legal claim, obtaining legal advice or conduct of a legal proceeding;

e) the processing is authorised by law and carried out by a competent public authority;

f) the processing is necessary in order to save the life of any person;

g) the processing is carried out for purposes of medical care or community welfare;

h) the processing is necessary to respond to a specific public health or humanitarian emergency and it is not reasonably possible to establish another legal basis for processing under this sub-article within a reasonable period of time;

i) the processing is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the data controller;

j) the processing is necessary for the purposes of the legitimate interests of the data controller or by a third party to which the personal data is validly disclosed, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject;

k) the processing is necessary for archiving purposes in the public interest, or for the purpose of historical, statistical or scientific research; or

l) the data subject has intentionally made such personal data public.

3. Further processing of personal data other than for the purpose for which it was originally collected shall be compatible with the purpose for which the data was collected.

4. Compatibility in sub-article 3 shall be assessed in light of:

a) the relationship between the original purpose and the purpose of the intended further processing;

b) the sensitivity of the personal data concerned;

c) the consequences and risks of the further processing;

d) how the personal data has been collected; and

e) the existence of appropriate safeguards.

5. The Authority may prescribe in regulations measures that must be applied to processing of sensitive personal data, categories of sensitive personal data, and classes of data subjects, having regard to:

a) the risk of significant harm that may be caused to a data subject or class of data subjects by the processing of a category of such sensitive personal data;

b) the reasonable expectation of confidentiality attached to such category of sensitive personal data; and

c) the adequacy of protection afforded to personal data generally.

Article 15: Purpose specification, data minimisation, retention and accuracy

A data controller shall ensure that personal data it processes is:

a) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

b) adequate, relevant and limited to what is the minimum necessary for such purposes;

c) retained for no longer than is necessary to achieve such purposes except where:

i. such retention is required or authorised by law; or

ii. the data subject has consented to such retention; and

d) accurate, complete, not misleading and, where necessary, kept up to date.

Article 16: Children and other persons lacking legal capacity

1. Where a data subject is a child or an individual otherwise lacking legal capacity, any consent that is required to be obtained shall be obtained from a parent or other appropriate legal representative.
2. A data controller may rely on consent provided by a child aged sixteen or more for the purposes of article 14(2)(a) in relation to the provision of information and services by electronic means at the individual request of the recipient.
3. The Authority may by regulation determine that sub-article 2 shall also apply to a child aged thirteen or more.
4. A data controller shall apply appropriate processes to verify the identity and age of a data subject and his representative, relationship to the data subject and consent.
5. For the purposes of sub-article 4, presentation of government approved identification documents shall be an appropriate mechanism.
6. Sub-article 1 does not apply when

a) the processing is necessary to protect the vital interests of the child or individual lacking the legal capacity to consent;

b) the processing is carried out for purposes of education or medical or social care and is undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or

c) the processing is necessary for proceedings before a court relating to the individual.

Article 17: Establishing data subject consent

1. A data controller shall bear the burden of proof for establishing a person's consent where any processing relies on consent under this Law.

Article 18: Provision of information to a data subject

1. A data controller shall ensure that a data subject is informed prior to collection of the personal data of:

   a) the identity of, and means of contacting, the data controller;

   b) the specific basis of processing under article 14(2) and the purposes of the processing;

   c) the identity of any other entity or person with which the personal data will be shared;

   d) data subjects' rights under Chapter IV and rights to lodge complaints with the Authority in accordance with article 31; and

   e) a description of any automated decision-making, including profiling, significance, envisaged and the likely consequence of such automated decision-making for the data subject.

1. Where the information provided for in sub-article 1 was not provided to the data subject before collection, the data controller shall ensure that it is provided as soon thereafter as possible.

2. Sub-articles 1 and 1 shall not apply if, but only to the extent that, compliance would be impossible or would involve a disproportionate effort or expense.

Article 19: Responsibility for data processors

1. A data controller shall keep a record of all data processors that process personal data with respect to which it is a data controller, including data processors engaged by other data processors.

2. A data controller shall take reasonable measures to ensure that any data processor that processes personal data with respect to which the former is a data controller:
    a) carries out its processing in a manner that ensures the data controller's compliance with this Law;
    b) provides all notifications, information and assistance reasonably required for the data controller to comply and demonstrate compliance with this Law;
    c) meets the requirements of article 24 as if it applied to data processors; and
    d) keeps a record and promptly notifies the data controller of any personal data breach, including the facts relating to a personal data breach, its effects and any remedial actions taken.
3. Reasonable measures under sub-article 2 include a written agreement between the data controller and each data processor it directly engages, including a contractual requirement in that agreement that the data processor shall ensure that all further data processors that may be engaged enter into a similar written agreement.
4. All references in this Law to processing of personal data by a data controller shall include processing by a data processor of any personal data with respect to which the former is the data controller, and the data controller shall be responsible for compliance of such processing with this Law.

CHAPTER IV—RIGHTS OF A DATA SUBJECT

Article 20: Rights of confirmation, access, correction and deletion

1. Subject to sub-article 1, a data subject has the right to obtain from a data controller for reasonable purposes, at no expense and without unreasonable delay:
    a) confirmation as to whether or not the data controller is processing personal data relating to the data subject and the source of such personal data;
    b) a copy of such personal data in a commonly used electronic format;
    c) correction, or if correction is not feasible or suitable, deletion of any such personal data that is inaccurate, out of date, incomplete or misleading; and
    d) deletion of any such personal data which the data controller is not entitled to retain.

1. If a data subject's request under sub-article 1 is manifestly unfounded or excessive, in particular because of its repetitive character, a data controller may charge a data subject a reasonable fee in relation to a request under sub-article 1 or refuse the request.
2. Any fee under sub-article 1 shall be set taking into account the administrative costs of providing the information or communication or taking the action requested.

Article 21: Right to withdraw consent

1. A data subject has the right to withdraw consent to processing previously given to a data controller.
2. A data controller shall ensure that it is as easy for the data subject to withdraw as to give consent, and that he or is informed of the consequences of doing so.

Article 22: Right to object

1. A data subject has the right to object:
   a) to the processing of personal data relating to the data subject based on article 14(2)i), j) or l) if such processing causes substantial unwarranted damage or distress; or
   b) in violation of the right under article 23 not to be subject to a decision based solely on automated processing, including profiling.
2. If a data subject validly objects to processing under sub-article 1, a data controller may no longer process such data unless a public interest or other legitimate grounds outweigh the unwarranted distress or damage.

Article 23: Right not to be subject to a decision based solely on automated processing

1. A data subject has the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject, except where such decisions are:
   a) necessary for the entering into or performance of a contract between the data subject and a data controller;
   b) authorized by a written law which establishes suitable measures to safeguard the fundamental rights and the interests of the data subject; or
   c) authorized by the consent of the data subject.

CHAPTER V—DATA SECURITY AND DATA IMPACT ASSESSMENTS

Article 24: Security, integrity and confidentiality of personal data

1. A data controller shall implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control including protections against accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access.
2. In implementing measures under sub-article 1, the data controller shall take into account:
    a) the amount and sensitivity of the personal data;
    b) the nature, degree and likelihood of harm to data subjects that could result from the loss, disclosure or other misuse of the personal data;
    c) the extent of the processing;
    d) the period of data retention; and
    e) the availability and cost of any technologies, tools or other measures to be implemented.
3. Measures implemented under sub-article 1 may include:
    a) pseudonymization or other methods of de-identification of personal data;
    b) encryption of personal data;
    c) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services;
    d) processes to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
    e) periodic assessments of risks to processing systems, services and transmission over electronic communications networks;
    f) regular testing, assessing and evaluation of the effectiveness of the measures implemented against current and evolving risks identified; and
    g) regular updating of the measures and introduction of new measures to address shortcomings in effectiveness and accommodate evolving risks.

Article 25: Data breach notifications

1. When a personal data breach has occurred with respect to personal data and is likely to result in a risk to the rights and freedoms of individuals, the data controller shall notify the Authority of the breach within seventy-two hours after having become aware of it.

2. The data controller may extend the seventy-two-hour period in sub-article 1 to accommodate the legitimate needs of law enforcement or as reasonably necessary to implement measures required to determine the scope of the breach.
3. If the data controller extends the period in accordance with sub-article 2, it shall inform the Authority of the grounds for such extension, including supporting evidence, within the seventy-two hour-period required in sub-article 1.
4. Subject to sub-article 5, when a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller shall also communicate the personal data breach to each affected data subject without undue delay in plain and clear language.
5. If a direct communication to the data subject under sub-article 4 would involve disproportionate effort or expense or is otherwise not feasible, the data controller may instead inform data subjects through one or more widely-used media sources.
6. In evaluating risk to the rights and freedoms of a data subject under sub-article 4, the data controller shall take into account:
    a) the likely effectiveness of any technical and administrative measures implemented to mitigate the likely harm resulting from the personal data breach;
    b) any subsequent measures taken to mitigate such risk; and
    c) the nature, scope and sensitivity of the personal data and vulnerability of data subjects involved.
7. The Authority may at any time make a public communication about a personal data breach if it considers the communications made by a data controller to data subjects under sub-article 4 inadequate.

Article 26: Contents of data breach notifications and communications

1. The personal data breach notifications and communications required to be made by a data controller under article 25 shall:
    a) set out the nature of the personal data breach including, where possible, the categories and approximate numbers of data subjects and personal data records concerned;
    b) communicate the name and contact details of a point of contact of the data controller where more information can be obtained;
    c) describe the likely consequences to affected data subjects of the personal data breach;

d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including any measures to mitigate its possible adverse effects; and

e) in the case of a communication made to affected data subjects or a public communication, provide advice about measures the affected data subject could take to mitigate effectively the possible adverse effects of the personal data breach.

2. To the extent that it is not possible to provide information under this article at the same time, the information may be provided in phases without undue further delay.

Article 27: Records of data breaches

1. Each data controller shall keep a record of all personal data breaches with respect to personal data processed by it, including the facts relating to the personal data breach, its effects and the remedial action taken in a manner that enables the Authority to verify compliance with this Chapter.

Article 28: Guidance from the Authority

1. The Authority shall issue guidance on the steps to be taken by data controllers to comply with the personal data breach notification and communication obligations in this Chapter.

Article 29: Data protection impact assessments

1. Where processing by a data controller of major importance is likely to result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes, a data controller of major importance shall:

   a) carry out a data protection impact assessment prior to the processing; and

   b) submit a data impact assessment report to the Authority prior to the processing.

2. The data controller of major importance shall consult the Authority prior to the processing if, notwithstanding the measures envisaged under sub-article 4d), the data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of a data subject.

3. The Authority shall issue guidelines on:

   a) carrying out data impact assessments; and

   b) the kinds of processing which require a data protection impact assessment pursuant to sub-article 1.

4. For purposes of this article, a "data protection impact assessment" is an assessment of the impact of the envisaged processing on the protection of personal data comprising:
    a) a systematic description of the envisaged processing and its purpose, including where applicable the legitimate interest justifying the processing;
    b) an assessment of the necessity and proportionality of the processing in relation to the purposes for which the personal data would be processed;
    c) an assessment of the risks to the rights and freedoms of data subjects; and
    d) the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Law.
5. The Minister may make regulations exempting categories of data controllers of major importance from some or all of the obligations under this article.
6. In determining any exemptions under sub-article 5, the Authority shall consider:
    a) the burden and proportionality of preparing a data protection impact assessment;
    b) the likelihood and gravity of risks to the rights and freedoms of data subjects; and
    c) other means of assessing and mitigating such risks.

CHAPTER VI—CROSS-BORDER TRANSFERS OF PERSONAL DATA

Article 30: Adequate level of protection for cross-border transfers of personal data

1. A data controller shall not transfer personal data to a country outside the Federal Republic of Somalia or international organisation unless one of the following conditions is met:
    a) the personal data shall be received solely within one or more countries, regions or specified sector within a country that affords an adequate level of protection;
    b) the recipient is an international organisation whose policies and administrative and technical measures afford an adequate level of protection;

c) the recipient is subject to a law, binding corporate rules, contractual clauses, code of conduct, certification mechanism or other measure that affords an adequate level of protection; or

d) one of the legal bases set forth in article 31 applies.

2. The adequacy of level of protection under sub-article 1 shall be assessed taking into account:

a) whether the form of protection upholds principles that are substantially similar to the conditions for processing of the personal data provided for in this Law, including in relation to the onward transfer of personal data to outside of the recipient's jurisdiction;

b) the availability of enforceable data subject rights, the ability of data subjects to enforce their rights through administrative or judicial redress, and the rule of law generally;

c) the existence and terms of any legally binding instrument between the Authority and a relevant public authority in the recipient country relating to data protection;

d) the access of a foreign public authority to personal data;

e) the existence of an effective data protection law in the jurisdiction where the recipient will receive the personal data;

f) the existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement powers in the jurisdiction where the recipient will receive the personal data; and

g) international commitments and conventions binding on the jurisdiction where the recipient will receive the personal data and its membership in any multilateral or regional organisations.

3. A data controller shall keep a record of the condition under sub-article 1 relied upon to permit a transfer of personal data to a country outside the Federal Republic of Somalia or an international organisation, including any assessment made under sub-article 2.

4. The Authority may:

a) issue rules and guidelines with respect to the assessment of adequacy of protection under sub-article 1 and the factors under sub-article 2;

b) designate any international organisation, country, region or specified sector within a country, law, binding corporate rules, contractual clauses, code of conduct, certification mechanism or other measure as affording or not affording adequate protection under sub-article 1;

c) provide guidance to a data controller on, and make a determination with respect to, the adequacy of protection afforded in relation to any specific transfer of personal data under sub-article 1; and

d) require any data controller to notify the Authority of the conditions relied upon under sub-article 1 for a transfer of personal data.

5. Whether or not the Authority makes any rule or guideline or designation under sub-article 4a) or b) shall not affect whether or not a data controller is in compliance with sub-article 1.

Article 31: Cross-border transfers in the absence of adequate protection

1. If none of the conditions in article 30(1)a), b) or c) apply, a data controller may nevertheless transfer personal data to a country outside of the Federal Republic of Somalia or an international organisation if:

   a) the data subject has given and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections;

   b) the processing is necessary for the entering into or performance of a contract with the data subject;

   c) the transfer is necessary for the entering into or performance of a contract made in the interest of the data subject between the data controller and a third party; or

   d) the transfer is for the benefit of the data subject and:

      i. it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

      ii. if it were reasonably practicable to obtain such consent, the data subject would likely give it.

2. Where a transfer of personal data to a country outside the Federal Republic of Somalia or an international organisation could not be based on a provision in article 30 or 31(1), the transfer may take place only if:

   a) the transfer is not repetitive;

   b) the transfer concerns only a limited number of data subjects;

   c) the transfer is necessary for the purposes of compelling legitimate interests pursued by the data controller which are not overridden by the interests or rights and freedoms of the data subject; and

   d) the data controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

3. In the case of a transfer made under sub-article 2, the data controller shall:

a) inform the Authority of the transfer; and

b) in addition to providing the information referred to in article 18, inform the data subject of the transfer and on the compelling legitimate interests pursued.

CHAPTER VII—REGISTRATION AND FEES

Article 32: Registration of data controllers of major importance

1. All data controllers of major importance shall register with the Authority within six months after qualifying as a data controller of major importance under this Law.
2. Registration under sub-article 1 shall be made by notifying the Authority of:
   a) its name and address and the name and contact information of its data protection officer;
   b) a description of the personal data with respect to which it is a data controller of major importance;
   c) the categories and number of data subjects to which the personal data relate;
   d) the purposes for which the personal data is or is intended to be processed;
   e) the categories of recipients to whom the personal data is or is intended to be disclosed;
   f) any international organisation or jurisdiction outside of the Federal Republic of Somalia to which the personal data is transferred or intended to be transferred;
   g) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data; and
   h) any other information required by the Authority.
3. A data controller of major importance shall update its registration annually.
4. The Authority shall maintain the currency of and publish on its website a register of data controllers of major importance that have duly registered with it under this article.
5. The General Manager may in a bylaw exempt a class of data controller of major importance from the registration requirement of this article where he or she considers such requirement to be unnecessary or disproportionate or outweighed by considerations in the public interest.

6. A data controller of major importance shall not be deemed to qualify as such for purposes of sub-article 1 until the date on which this Law comes into force.

Article 33: Fees and levies

1. The General Manager may in a bylaw prescribe annual fees or levies which shall be paid by data controllers of major importance in order to meet the costs of the Authority under this Law.
2. The levels of fees and levies may vary according to class or size of data controllers of major importance.
3. The Government, statutory bodies and any other body appointed by the Government to carry out public functions shall not be subject to the annual fees or levies under sub-article 1.

Article 34: Designation of data protection officers

1. A data controller of major importance shall designate a data protection officer with expert knowledge of data protection law and practices and the ability to carry out the tasks referred to in sub-article 3.
2. The data protection officer may be an employee or engaged by service contract.
3. The data protection officer shall have the tasks of:
   a) advising the data controller of its obligations under this Law;
   b) monitoring compliance with this Law and related policies of the data controller; and
   c) acting as the contact point for the Authority on issues relating to processing of personal data.

CHAPTER VIII—ENFORCEMENT

Article 35: Complaints

1. A data subject who is aggrieved by any act or omission of a data controller resulting in a violation of this Law or any regulations, rules or other subsidiary legislation or orders may lodge a complaint with the Authority.
2. The Authority shall admit any complaint referred to it where it appears to the Authority that:
   a) the complainant has an interest in the matter to which the complaint relates; and

b) the complaint is not frivolous or vexatious.

3. The Authority shall establish a unit or department that shall receive and process complaints from data subjects and conduct investigations.

Article 36: Investigations

1. The Authority may initiate an investigation pursuant to a complaint it has admitted or of its own accord where it has reason to believe a data controller has violated or is likely to violate this Law or any regulations, rules or other subsidiary legislation or orders.
2. The Authority may, for the purpose of an investigation, order any person to—
   a) attend at a specific time and place for the purpose of being examined orally in relation to a complaint;
   b) produce such document, record or article as may be required with respect to any matter relevant to the investigation, which the person is not prevented by any other written law from disclosing; or
   c) furnish a statement in writing made under oath or an affirmation setting out all information which may be required under the order.
3. Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Authority may require the person named to produce or give access to it in a form in which it is visible and legible in a structured, commonly used and machine-readable format.

Article 37: Orders of the Authority

1. If the Authority, after completing an investigation under article 36, is satisfied that a data controller has violated any provision of this Law, or any regulation, rule or other subsidiary legislation made hereunder, it may make any appropriate order requiring the data controller to:
   a) stop or refrain from doing an act which is in violation of this Law, including stopping or refraining from processing that is the subject of the order;
   b) take reasonable action to compel a data processor to stop or refrain from processing as required to ensure the data controller's compliance;
   c) remedy the violation;
   d) pay compensation to a data subject who suffers injury, loss or harm as a result of a violation;
   e) account for the profits made out of the violation; or

f) pay an administrative penalty of up to [US one million dollars] or its equivalent in Somali currency.

2. Any order made by the Authority under sub-article 1 shall be proportionate to and shall take into account:
   a) the gravity of the violation and its repetitive nature;
   b) the data controller's efforts to comply and provide information to the Authority and data subjects; and
   c) the resulting harm and risk to the rights and freedoms of data subjects.

Article 38: Failure to comply with an order of the Authority

1. A data controller who fails to comply with any order made under article 36 that is not the subject of a duly made and ongoing appeal under article 39 commits an offence for which such data controller is liable to a fine of [US one million dollars] or its equivalent in Somali currency and imprisonment for [two] years.
2. Liability for a fine under sub-article 1 does not release or reduce any liability arising from an order made under article 37.

Article 39: Appeal of an order of the Authority

1. A data subject, data controller or other interested person who is not satisfied with an order of the Authority may apply to the Supreme Court within thirty days after the date the order was made for judicial review thereof.

Article 40: Civil remedies

1. A data subject who suffers injury, loss or harm as a result of a violation of this Law by a data controller, or a consumer organisation acting on behalf of such a data subject or multiple data subjects, may recover damages by way of civil proceedings in the appropriate court from such data controller.

CHAPTER IX—MISCELLANEOUS

Article 41: Power to issue regulations

1. The Authority shall have the power to issue regulations published in the Official Bulletin elaborating on the provisions of this Law.
2. Without prejudice to the generality of sub-article 1, the regulations may provide for:
   a) the financial management of the affairs of the Authority;

b) the protection of personal data and data subjects;

c) the manner in which the Authority may exercise any power or perform any duty or function under this Law;

d) any matter that under this Law that is required or permitted to be prescribed in regulations; or

e) any matter that the Authority considers necessary or expedient to give effect to the objectives of this Law.

Article 42: Repeal

1. Any law which is inconsistent with this Law shall, to the extent of the inconsistency, be void.

Article 43: Coming into force

1. This law shall come into force when it is adopted by the Federal Parliament of Somalia, promulgated by the President of the Federal Republic of Somalia and published in the Official Bulletin.