No. 2019



THE REPUBLIC OF KENYA

HIS EXCELLENCY THE PRESIDENT

UHURU KENYATTA

I assent

President

, 2019

An Act of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes

THE DATA PROTECTION ACT, 2019

No. of 2019

ARRANGEMENT OF SECTIONS

Sections

PART I—PRELIMINARY

1. —Short title.
2. —Interpretation.
3. —Object and purpose of this Act.
4. —Application.

PART II—ESTABLISHMENT OF THE OFFICE OF THE DATA PROTECTION COMMISSIONER

5. —Establishment of the Office.
6. —Appointment of the Data Commissioner.
7. —Qualifications of the Data Commissioner.
8. —Functions of the Data Commissioner.
9. —Powers of the Office.
10. —Delegation by the Data Commissioner.
11. —Vacancy in the Office of the Data Commissioner.
12. —Removal of the Data Commissioner from office.
13. —Staff of the Office.
14. —Remuneration of the Data Commissioner and staff.
15. —Oath of Office.
16. —Confidentiality agreements.
17. —Protection from personal liability.

PART III—REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

18. —Registration of data controllers and data Processors.
19. —Application for registration.
20. —Duration of the registration certificate.
21. —Register of data controllers and data processors.

22. —Cancellation or variation of the certificate.

23. —Compliance and audit.

24. —Designation of the Data Protection Officer.

PART IV—PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

25. —Principles of personal data protection.

26. —Rights of a data subject.

27. —Exercise of rights by data subject.

28. —Collection of personal data.

29. —Duty to notify.

30. —Lawful processing of personal data.

31. —Data protection impact assessment.

32. —Conditions for consent.

33. —Processing of personal data relating to a child.

34. —Restriction on processing.

35. —Automated individual decision making.

36. —Objecting to processing.

37. —processing for direct marketing.

38. —Right to data portability.

39. —Limitation to retention of personal data.

40. —Right of rectification and erasure.

41. —Data protection by design or default.

42. —Particulars of determining organisational measures.

43. —Notification and communication of breach.

PART V—GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

44. —Processing of sensitive personal data.

45. —Permitted grounds for processing sensitive personal data.

46. —Personal data relating to health.

47. —Further categories of sensitive personal data.

PART VI—TRANSFER OF PERSONAL DATA OUTSIDE KENYA

48. —Conditions for transfer out of Kenya.

49. —Safeguards prior to transfer of personal data out of Kenya.

50. —Processing through a data server or centre in Kenya.

PART VII—EXEMPTIONS

51. —General exemptions.

52. —Journalism, literature and art.

53. —Research, history and statistics.

54. —Exemptions by the Data Commissioner.

55. —Data-sharing code.

PART VIII—ENFORCEMENT PROVISIONS

56. —Complaints to the Data Commissioner.

57. —Investigation of complaints.

58. —Enforcement notices.

59. —Power to seek assistance.

60. —Power of entry and search.

61. —Obstruction of the Data Commissioner.

62. —Penalty notices.

63. —Administrative fines.

64. – Right of appeal.

65. —Compensation of data subject.

66. —Preservation Order.

PART IX—FINANCIAL PROVISIONS

67. —Funds of the Office.

68. —Annual estimates.

69. —Accounts and Audit.

70. —Annual report.

PART X —PROVISIONS ON DELEGATED POWERS

71. —Regulations.

PART XI—MISCELLANEOUS PROVISIONS

72. —Offences of unlawful disclosure of Personal Data.

73. —General penalty.

74. —Codes, guidelines and certification.

75. —Consequential amendments.

THE DATA PROTECTION ACT, 2019

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes

ENACTED by Parliament of Kenya, as follows—

PART I—PRELIMINARY

Short title.

1. This Act may be cited as the Data Protection Act, 2019.

Interpretation.

2. In this Act, unless the context otherwise requires—

"anonymisation" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

"biometric data'' means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

"Cabinet Secretary" means the Cabinet Secretary responsible for matters relating to information, communication and technology;

"consent" means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject;

"data" means information which—

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system;

(d) where it does not fall under paragraphs (a) (b) or (c), forms part of an accessible record; or

(e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

"Data Commissioner" means the person appointed under section 6;

"data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;

"data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"data subject" means an identified or identifiable natural person who is the subject of personal data;

"encryption" means the process of converting the content of any readable data using technical means into coded form;

"filing system" means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"health data" means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services;

"identifiable natural person" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

"national security organs" has the meaning assigned to it under Article 239 of the Constitution;

"person" has the meaning assigned to it under Article 260 of the Constitution;

"personal data" means any information relating to an identified or identifiable natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"Office" means the office of the Data Protection Commissioner;

"processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as—

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements;

"pseudonymisation" 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, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"register" means the register kept and maintained by the Data Commissioner under section 21;

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject; and

"third Party" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data;

Object and purpose of this Act.

3. The object and purpose of this Act is—

(a) to regulate the processing of personal data;

(b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25;

(c) to protect the privacy of individuals;

(d) to establish the legal and institutional mechanism to protect personal data; and

(e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

Application.

4. This Act applies to the processing of personal data —

(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means:

Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;

(b) by a data controller or data processor who—

(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or

(ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.

PART II—ESTABLISHMENT OF THE OFFICE OF DATA PROTECTION COMMISSIONER

Establishment of the Office.

5. (1) There is established the office of the Data Protection Commissioner which shall be a body corporate with perpetual succession and a common seal and shall in its corporate name, be capable of—

(a) suing and being sued;

(b) taking, purchasing or otherwise acquiring, holding, charging or disposing of movable and immovable property;

(c) entering into contracts; and

(d) doing such other legal acts necessary for the proper performance of the functions of the Office.

(2) The Office is designated as a State Office in accordance with Article 260(q) of the Constitution.

(3) The Office shall comprise the Data Commissioner as its head and accounting officer, and other staff appointed by the Data Commissioner.

(4) The Office shall ensure reasonable access to its services in all parts of the Republic.

(5) The Data Commissioner shall in consultation with the Cabinet Secretary, establish such directorates as may be necessary for the better carrying of the functions of the Office.

Appointment of the Data Commissioner.

6. (1) The Public Service Commission shall, whenever a vacancy arises in the position of the Data Commissioner, initiate the recruitment process.

(2) The Public Service Commission shall, within seven days of being notified of a vacancy under subsection (1), invite applications from persons who qualify for nomination and appointment for the position of the Data Commissioner.

(3) The Public Service Commission shall within twenty-one days of receipt of applications under subsection (2)—

(a) consider the applications received to determine their compliance with this Act;

(b) shortlist qualified applicants;

(c) publish and publicise the names of the applicants and the shortlisted applicants;

(d) conduct interviews of the shortlisted persons in an open and transparent process;

(e) nominate three qualified applicants in the order of merit for the position of Data Commissioner; and

(f) submit the names of the persons nominated under paragraph (e) to the President.

(4) The President shall nominate and, with approval of the National Assembly, appoint the Data Commissioner.

Qualifications of Data Commissioner.

7. (1) A person shall be qualified for appointment as the Data Commissioner if that person—

(a) holds a degree from a university recognized in Kenya in—

(i) data science;

(ii) law;

(iii) information technology; or

(iv) any other related field;

(b) has knowledge and relevant experience of not less than ten years;

(c) meets the requirements of Chapter Six of the Constitution; and

(d) holds a master's degree.

(2) The Data Commissioner shall be appointed for a single term of six years and shall not be eligible for a re-appointment.

Functions of the Office.

8. (1) The Office shall—

(a) oversee the implementation of and be responsible for the enforcement of this Act;

(b) establish and maintain a register of data controllers and data processors;

(c) exercise oversight on data processing operations, either of own motion or at the request of a data

subject, and verify whether the processing of data is done in accordance with this Act;

(d) promote self-regulation among data controllers and data processors;

(e) conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;

(f) receive and investigate any complaint by any person on infringements of the rights under this Act;

(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;

(h) carry out inspections of public and private entities with a view to evaluating the processing of personal data;

(i) promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;

(j) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals; and

(k) perform such other functions as may be prescribed by any other law or as necessary for the promotion of object of this Act.

(2) The Office of the Data Commissioner may, in the performance of its functions collaborate with the national security organs.

(3) The Data Commissioner shall act independently in exercise of powers and carrying out of functions under this Act.

Powers of the Office.

9. (1) The Data Commissioner shall have power to—

(a) conduct investigations on own initiative, or on the basis of a complaint made by a data subject or a third party;

(b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate;

(c) facilitate conciliation, mediation and negotiation on disputes arising from this Act;

(d) issue summons to a witness for the purposes of investigation;

(e) require any person that is subject to this Act to provide explanations, information and assistance in person and in writing;

(f) impose administrative fines for failures to comply with this Act;

(g) undertake any activity necessary for the fulfilment of any of the functions of the Office; and

(h) exercise any powers prescribed by any other legislation.

(2) The Data Commissioner may enter into association with other bodies or organisations within and outside Kenya as appropriate in furtherance of the object of this Act.

Delegation by the Data Commissioner.

10. The Data Commissioner may, subject to such conditions as the Data Commissioner may impose, delegate any power conferred under this Act or any other written law to a regulator established through an Act of Parliament.

Vacancy in the Office of the Data Commissioner.

11. The Office of the Data Commissioner shall become vacant, if the Data Commissioner—

(a) dies;

(b) resigns from office by notice in writing addressed to the President;

(c) is convicted of an offence and sentenced to imprisonment for a term exceeding six months without the option of a fine;

(d) is removed from office on the grounds of—

(i) inability to perform the functions of office arising from mental or physical infirmity;

(ii) non-compliance with Chapter Six of the Constitution;

(iii) bankruptcy;

(iv) incompetence; or

(v) gross misconduct.

Removal of the Data Commissioner.

12. (1) A person desiring the removal of Data Commissioner on any ground specified under section 11 (d) may present a complaint to the Public Service Commission setting out the alleged facts constituting that ground.

(2) Subject to Article 47 of the Constitution, the Public Service Commission shall consider the complaint and, if satisfied that the complaint discloses a ground under section 11 (d), shall—

(a) investigate the matter expeditiously;

(b) report on the facts; and

(c) make a recommendation to the Cabinet Secretary.

(3) Prior to any action under sub-section (2), the Data Commissioner shall be—

(a) informed, in writing, of the reasons for the intended removal; and

(b) offered an opportunity to put in a defence against any such allegations.

Staff of the Office.

13. The Data Commissioner shall in consultation with the Public Service Commission, appoint such number of staff as may be necessary for the proper and efficient discharge of the functions under this Act or any other relevant law.

Remuneration of the Data Commissioner and staff.

14. The Data Commissioner and staff of the Office shall be paid such remuneration or allowances as the Salaries and Remuneration Commission may advise.

Oath of office.

15. The Data Commissioner shall take the oath set out in the First Schedule on appointment.

Confidentiality agreement.

16. The Data Commissioner, or any staff of the Office, shall not, unless with lawful authority, disclose any information obtained for the purposes of this Act.

Protection from personal liability.

17. The Data Commissioner or any staff of the Office shall not be held liable for having performed any of their functions in good faith and in accordance with this Act.

PART III— REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Registration of data controllers and data processors.

18. (1) Subject to sub-section (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner.

(2) The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider—

(a) the nature of industry;

(b) the volumes of data processed;

(c) whether sensitive personal data is being processed; and

(d) any other criteria the Data Commissioner may specify.

Application for registration.

19. (1) A data controller or data processor required to register under section 18 shall apply to the Data Commissioner.

(2) An application under sub-section (1) shall provide the following particulars—

(a) a description of the personal data to be processed by the data controller or data processor;

(b) a description of the purpose for which the personal data is to be processed;

(c) the category of data subjects, to which the personal data relates;

(d) contact details of the data controller or data processor;

(e) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data;

(f) any measures to indemnify the data subject from unlawful use of data by the data processor or data controller; and

(g) any other details as may be prescribed by the Data Commissioner.

(3) A data controller or data processor who knowingly supplies any false or misleading detail under sub-section (1) commits an offence.

(4) The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.

(5) A data controller or data processor shall notify the Data Commissioner of a change in any particular outlined under subsection (2).

(6) On receipt of a notification under sub-section (5), the Data Commissioner shall amend the respective entry in the Register.

(7) A data controller or data processor who fails to comply with the provisions of this section commits an offence.

Duration of the registration certificate.

20. A registration certificate issued under section 19 shall be valid for a period determined at the time of the application after taking into account the need for the certificate, and the holder may apply for a renewal of the certificate after expiry of the certificate.

Register of data controllers and data processors.

21. (1) The Data Commissioner shall keep and maintain a register of the registered data controllers and data processors.

(2) The Data Commissioner may, at the request of a data controller or data processor, remove any entry in the register which has ceased to be applicable.

(3) The register shall be a public document and available for inspection by any person.

(4) A person may request the Data Commissioner for a certified copy of any entry in the register.

Cancellation or variation of the certificate.

22. The Data Commissioner may, on issuance of a notice to show cause, vary terms and conditions of the certificate of registration or cancel the registration where—

(a) any information given by the applicant is false or misleading; or;

(b) the holder of the registration certificate, without lawful excuse, fails to comply with any requirement of this Act.

Compliance and audit.

23. The Data Commissioner may carry out periodical audits of the processes and systems of the data controllers or data processors to ensure compliance with this Act.

Designation of the Data Protection Officer.

24. (1) A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where—

(a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;

(b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects; or

(c) the core activities of the data controller or the data processor consist of processing of sensitive categories of personal data.

(2) A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.

(3) A group of entities may appoint a single data protection officer provided that such officer is accessible by each entity.

(4) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures.

(5) A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

(6) A data controller or data processor shall publish the contact details of the data protection officer on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

(7) A data protection officer shall—

(a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;

(b) ensure on behalf of the data controller or data processor that this Act is complied with;

(c) facilitate capacity building of staff involved in data processing operations;

(d) provide advice on data protection impact assessment; and

(e) co-operate with the Data Commissioner and any other authority on matters relating to data protection.

PART IV—PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

Principles of data protection.

25. Every data controller or data processor shall ensure that personal data is—

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

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

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

(g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

(h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Rights of a data subject.

26. A data subject has a right —

(a) to be informed of the use to which their personal data is to be put;

(b) to access their personal data in custody of data controller or data processor;

(c) to object to the processing of all or part of their personal data;

(d) to correction of false or misleading data; and

(e) to deletion of false or misleading data about them.

Exercise of rights of data subjects.

27. A right conferred on a data subject may be exercised—

(a) where the data subject is a minor, by a person who has parental authority or by a guardian;

(b) where the data subject has a mental or other disability, by a person duly authorised to act as their guardian or administrator; or

(c) in any other case, by a person duly authorised by the data subject.

Collection of personal data.

28. (1) A data controller or data processor shall collect personal data directly from the data subject.

(2) Despite sub-section (1), personal data may be collected indirectly where—

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public;

(c) the data subject has consented to the collection from another source;

(d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source;

(e) the collection from another source would not prejudice the interests of the data subject;

(f) collection of data from another source is necessary—

(i) for the prevention, detection, investigation, prosecution and punishment of crime;

(ii) for the enforcement of a law which imposes a pecuniary penalty; or

(iii) for the protection of the interests of the data subject or another person.

(3) A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.

Duty to notify.

29. A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject of —

(a) the rights of data subject specified under section 26;

(b) the fact that personal data is being collected;

(c) the purpose for which the personal data is being collected;

(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;

(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;

(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and

(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

Lawful processing of personal data.

30. (1) A data controller or data processor shall not process personal data, unless—

(a) the data subject consents to the processing for one or more specified purposes; or

(b) the processing is necessary—

(i) for the performance of a contract to which the data subject is a party or in order to take

steps at the request of the data subject before entering into a contract;

(ii) for compliance with any legal obligation to which the controller is subject;

(iii) in order to protect the vital interests of the data subject or another natural person;

(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(v) the performance of any task carried out by a public authority;

(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;

(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

(viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

(2) Further processing of personal data shall be in accordance with the purpose of collection.

(3) A data controller who contravenes the provisions of sub-section (1) commits an offence.

Data protection impact assessment.

31. (1) Where a processing operation 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 or data processor shall, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment shall include the following—

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the

legitimate interest pursued by the data controller or data processor;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects;

(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 Act, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

(3) The data controller or data processor shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.

(4) For the purposes of this section, a "data protection impact assessment" means an assessment of the impact of the envisaged processing operations on the protection of personal data.

(5) The data impact assessment reports shall be submitted sixty days prior to the processing of data.

(6) The Data Commissioner shall set out guidelines for carrying out an impact assessment under this section.

Conditions of consent.

32. (1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) The withdrawal of consent under sub-section (2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a

service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Processing of personal data relating to a child.

33. (1) Every data controller or data processor shall not process personal data relating to a child unless—

(a) consent is given by the child's parent or guardian; and

(b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.

(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of—

(a) available technology;

(b) volume of personal data processed;

(c) proportion of such personal data likely to be that of a child;

(d) possibility of harm to a child arising out of processing of personal data; and

(e) such other factors as may be specified by the Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).

Restrictions on processing.

34. (1) A data controller or data processor shall, at the request of a data subject, restrict the processing of personal data where—

(a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;

(b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise or defence of a legal claim;

(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(d) data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

(2) Where processing of personal data is restricted under this section—

(a) the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) the data controller shall inform the data subject before withdrawing the restriction on processing of the personal data.

(3) The data controller or data processor shall implement mechanisms to ensure that time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, is observed.

Automated individual decision making.

35. (1) Every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.

(2) Sub-section (1) shall not apply where the decision is—

(a) necessary for entering into, or performing, a contract between the data subject and a data controller;

(b) authorised by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) based on the data subject's consent.

(3) Where a data controller or data processor takes a decision, which produces legal effects or significantly

affects the data subject based solely on automated processing—

(a) the data controller or data processor must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and

(b) the data subject may, after a reasonable period of receipt of the notification, request the data controller or data processor to—

(i) reconsider the decision; or

(ii) take a new decision that is not based solely on automated processing.

(4) A data controller or data processor, upon receipt of a request under sub-section (3), shall within a reasonable period of time—

(a) consider the request, including any information provided by the data subject that is relevant to it;

(b) comply with the request; and

(c) by notice in writing inform the data subject of—

(i) the steps taken to comply with the request; and

(ii) the outcome of complying with the request.

(5) The Cabinet Secretary may by Regulations make such further provision to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of decisions based solely on automated processing.

Objecting to processing.

36. A data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim.

Commercial use of data.

37. (1) A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person—

(a) has sought and obtained express consent from a data subject; or

(b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

(3) The Cabinet Secretary, in consultation with the Data Commissioner, may prescribe practice guidelines for commercial use of personal data in accordance with this Act.

Right to data portability.

38. (1) A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit the data obtained under sub-section (1), to another data controller or data processor without any hindrance.

(3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.

(4) Where data controller or data processor declines to comply with a request under sub-section (3), the Data Commissioner may make a determination on the technical capacity of the data controller or data processor.

(5) The right under this section shall not apply in circumstances where—

(a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or

(b) it may adversely affect the rights and freedoms of others.

(6) A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of thirty days.

(7) Where the portability request is complex or numerous, the period under sub-section (6) may be extended for a further period as may be determined in consultation with the Data Commissioner.

Limitation to retention of personal data.

39. (1) A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is —

(a) required or authorised by law;

(b) reasonably necessary for a lawful purpose;

(c) authorised or consented by the data subject; or

(d) for historical, statistical, journalistic literature and art or research purposes.

(2) A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under sub-section (1) in a manner as may be specified at the expiry of the retention period.

Right of rectification and erasure.

40. (1) A data subject may request a data controller or data processor —

(a) to rectify without undue delay personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading; or

(b) to erase or destroy without undue delay personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(2) Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested—

(a) the rectification of such personal data in their possession or under their control that is inaccurate, out-dated, incomplete or misleading; or

(b) the erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(3) Where a data controller or data processor is required to rectify or erase personal data under sub-section (1), but the personal data is required for the purposes of evidence, the data controller or data processor shall, instead

of erasing or rectifying, restrict its processing and inform the data subject within a reasonable time.

Data protection by design or by default.

41. (1) Every data controller or data processor shall implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner; and

(b) to integrate necessary safeguards for that purpose into the processing.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing.

(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration—

(a) the amount of personal data collected;

(b) the extent of its processing;

(c) the period of its storage;

(d) its accessibility; and

(e) the cost of processing data and the technologies and tools used.

(4) To give effect to this section, the data controller or data processor shall consider measures such as—

(a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;

(b) to establish and maintain appropriate safeguards against the identified risks;

(c) to the pseudonymisation and encryption of personal data;

(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) to verify that the safeguards are effectively implemented; and

(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.

Particulars of determining organisational measures.

42. (1) In determining the appropriate measures referred to in section 41, in particular, where the processing involves the transmission of data over an information and communication network, a data controller shall have regard to—

(a) the state of technological development available;

(b) the cost of implementing any of the security measures;

(c) the special risks that exist in the processing of the data; and

(d) the nature of the data being processed.

(2) Where a data controller is using the services of a data processor—

(a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of organisational measures for the purpose of complying with section 41 (1); and

(b) the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

(3) Where a data processor processes personal data other than as instructed by the data controller, the data processor shall be deemed to be a data controller in respect of that processing.

(4) A data controller or data processor shall take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor, complies with the relevant security measures.

Notification and communication of breach.

43. (1) Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall—

(a) notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and

(b) subject to subsection (3), communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.

(2) Where the notification to the Data Commissioner is not made within seventy-two hours, the notification shall be accompanied by reasons for the delay.

(3) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller without delay and where reasonably practicable, within forty-eight hours of becoming aware of such breach.

(4) The data controller may delay or restrict communication referred to under subsection (1) (b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

(5) The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including —

(a) description of the nature of the data breach;

(b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;

(c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and

(e) the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.

(6) The communication of a breach to the data subject shall not be required where the data controller or data

processor has implemented appropriate security safeguards which may include encryption of affected personal data.

(7) Where and to the extent that it is not possible to provide all the information mentioned in subsection (5) at the same time, the information may be provided in phases without undue delay.

(8) The data controller shall record the following information in relation to a personal data breach—

(a) the facts relating to the breach;

(b) its effects; and

(c) the remedial action taken.

PART V— GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

Processing of sensitive personal data.

44. No category of sensitive personal data shall be processed unless section 25 applies to that processing.

Permitted grounds for processing sensitive personal data.

45. Without prejudice to section 44, sensitive personal data of a data subject may be processed where—

(a) the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that—

(i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and

(ii) the personal data is not disclosed outside that body without the consent of the data subject;

(b) the processing relates to personal data which is manifestly made public by the data subject; or

(c) processing is necessary for—

(i) the establishment, exercise or defence of a legal claim;

(ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or

(iii) protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

Personal data relating to health.

46. (1) Personal data relating to the health of a data subject may only be processed—

(a) by or under the responsibility of a health care provider; or

(b) by a person subject to the obligation of professional secrecy under any law.

(2) The condition under subsection (1) is met if the processing—

(a) is necessary for reasons of public interest in the area of public health; or

(b) is carried out by another person who in the circumstances owes a duty of confidentiality under any law.

Further categories of sensitive personal data.

47. (1) The Data Commissioner may prescribe further categories of personal data which may be classified as sensitive personal data.

(2) Where categories of personal data have been specified as sensitive personal data under subsection (1), the Data Commissioner may specify any further grounds on which such specified categories may be processed, having regard—

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

(b) to the expectation of confidentiality attached to such category of personal data;

(c) to whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and

(d) to the adequacy of protection afforded by ordinary provisions applicable to personal data.

(3) The Data Commissioner may specify other categories of personal data, which may require additional safeguards or restrictions.

PART VI —TRANSFER OF PERSONAL DATA OUTSIDE KENYA

Conditions for transfer out of Kenya.

48. A data controller or data processor may transfer personal data to another country only where—

(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;

(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;

(c) the transfer is necessary—

(i) for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) 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; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Safeguards prior to transfer of personal data out of Kenya.

49. (1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

(2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests.

(3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

Processing through a data server or data centre in Kenya.

50. The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.

PART VII— EXEMPTIONS

General exemptions.

51. (1) Nothing in this Part shall exempt any data controller or data processor from complying with data protection principles relating to lawful processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data.

(2) The processing of personal data is exempt from the provisions of this Act if—

(a) it relates to processing of personal data by an individual in the course of a purely personal or household activity;

(b) if it is necessary for national security or public interest; or

(c) disclosure is required by or under any written law or by an order of the court.

Journalism, literature and art.

52. (1) The principles of processing personal data shall not apply where—

(a) processing is undertaken by a person for the publication of a literary or artistic material;

(b) data controller reasonably believes that publication would be in the public interest; and

(c) data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

(2) Subsection (1)(b) shall only apply where it can be demonstrated that the processing is in compliance with any

self-regulatory or issued code of ethics in practice and relevant to the publication in question.

(3) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Journalism, Literature and Art.

Research, history and statistics.

53. (1) The further processing of personal data shall be compatible with the purpose of collection if the data is used for historical, statistical or research purposes and the data controller or data processor shall ensure that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

(2) The data controller or data processor shall take measures to establish appropriate safeguards against the records being used for any other purposes.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if—

(a) data is processed in compliance with the relevant conditions; and

(b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

(4) The Data Commissioner shall prepare a code of practice containing practical guidance in relation to the processing of personal data for purposes of Research, History and Statistics.

Exemptions by the Data Commissioner.

54. The Data Commissioner may prescribe other instances where compliance with certain provisions of this Act may be exempted.

Data-sharing code

55. (1) The Data Commissioner may issue a data sharing code which shall contain—

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation; and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) The data sharing code under subsection (1) shall specify on the lawful exchange of personal data between government departments or public sector agencies.

PART VIII—ENFORCEMENT PROVISIONS

Complaints to the Data Commissioner.

56. (1) A data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner in accordance with this Act.

(2) A person who intends to lodge a complaint under this Act shall do so orally or in writing.

(3) Where a complaint made under subclause (1) is made orally, the Data Commissioner shall cause the complaint to be recorded in writing and the complaint shall be dealt with in accordance with such procedures as the Data Commissioner may prescribe.

(4) A complaint lodged under subclause (1) shall contain such particulars as the Data Commissioner may prescribe.

(5) A complaint made to the Data Commissioner shall be investigated and concluded within ninety days.

Investigation of complaints.

57. (1) The Data Commissioner may, for the purpose of the investigation of a complaint, order any person to—

(a) attend at a specified time and place for the purpose of being examined orally in relation to the complaint;

(b) produce such book, 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 enactment from disclosing; or

(c) furnish a statement in writing made under oath or on affirmation setting out all information which may be required under the notice.

(2) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Data Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(3) A person who, without reasonable excuse, fails or refuses to comply with a notice, or who furnishes to the Data Commissioner any information which the person knows to be false or misleading, commits an offence.

Enforcement notices.

58. (1) Where the Data Commissioner is satisfied that a person has failed, or is failing, to comply with any provision of this Act, the Data Commissioner may serve an enforcement notice on that person requiring that person to take such steps and within such period as may be specified in the notice.

(2) An enforcement notice served under subsection (1) shall—

(a) specify the provision of this Act which has been, is being or is likely to be, contravened;

(b) specify the measures that shall be taken to remedy or eliminate the situation which makes it likely that a contravention will arise;

(c) specify a period which shall not be less than twenty-one days within which those measures shall be implemented; and

(d) state any right of appeal.

(3) Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

Power to seek assistance.

59. For the purpose of gathering information or for any investigation under this Act, the Data Commissioner may seek the assistance of such person or authority as they deem fit and as is reasonably necessary to assist the Data Commissioner in the discharge of their functions.

Power of entry and search.

60. The Data Commissioner, upon obtaining a warrant from a Court, may enter and search any premises for the purpose of discharging any function or exercising any power under this Act.

Obstruction of Data Commissioner.

61. A person who, in relation to the exercise of a power conferred by section 9—

(a) obstructs or impedes the Data Commissioner in the exercise of their powers;

(b) fails to provide assistance or information requested by the Data Commissioner;

(c) refuses to allow the Data Commissioner to enter any premises or to take any person with them in the exercise of their functions;

(d) gives to the Data Commissioner any information which is false or misleading in any material aspect,

commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

Penalty notices.

62. (1) If the Data Commissioner is satisfied that a person has failed or is failing as described in section 58, the Data Commissioner may issue a penalty notice requiring the person to pay to the Office of the Data Commissioner an amount specified in the notice.

(2) In deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Data Commissioner shall, so far as relevant, have regard—

(a) to the nature, gravity and duration of the failure;

(b) to the intentional or negligent character of the failure;

(c) to any action taken by the data controller or data processor to mitigate the damage or distress suffered by data subjects;

(d) to the degree of responsibility of the data controller or data processor, taking into account technical and organisational measures;

(e) to any relevant previous failures by the data controller or data processor;

(f) to the degree of co-operation with the Data Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) to the categories of personal data affected by the failure;

(h) to the manner in which the infringement became known to the Data Commissioner, including whether, and if so to what extent, the data controller or data processor notified the Data Commissioner of the failure;

(i) to the extent to which the data controller or data processor has complied with previous enforcement notices or penalty notices;

(j) to adherence to approved codes of conduct or certification mechanisms;

(k) to any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) to whether the penalty would be effective, proportionate and dissuasive.

Administrative fines.

63. In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

Right of appeal.

64. A person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court.

Compensation to a data subject.

65. (1) A person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor.

(2) Subject to subsection (1)—

(a) a data controller involved in processing of personal data is liable for any damage caused by the processing; and

(b) a data processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the Act specifically directed at data processors; or

(ii) has acted outside, or contrary to, the data controller's lawful instructions.

(3) A data controller or data processor is not liable in the manner specified in subsection (2) if the data controller

or data processor proves that they are not in any way responsible for the event giving rise to the damage.

(4) In this section, "damage" includes financial loss and damage not involving financial loss, including distress.

Preservation Order.

66. The Data Commissioner may apply to a court for a preservation order for the expeditious preservation of personal data including traffic data, where there is reasonable ground to believe that the data is vulnerable to loss or modification.

PART IX—FINANCIAL PROVISIONS

Funds of the Office.

67. The funds and assets of the Office shall consist of—

(a) monies allocated by the National Assembly for purposes of the Office;

(b) any grants, gifts, donations or other endowments given to the Office; and

(c) such funds as may vest in or accrue to the Office in the performance of its functions under this Act or any other written law.

Annual estimates.

68. (1) At least three months before the commencement of each financial year, the Data Commissioner shall cause to be prepared estimates of the revenue and expenditure of the Office for that year.

(2) The annual estimates shall make provision for all the estimated expenditure of the Office for the financial year concerned and in particular shall provide for—

(a) the payment of salaries, allowances and other charges in respect of the staff of the Office;

(b) the payment of pensions, gratuities and other charges in respect of retirement benefits which are payable out of the finances of the Office;

(c) the acquisition, maintenance, repair and replacement of the equipment and other movable property of the Office;

(d) funding of training, research and development of activities of the Office;

(e) the creation of such reserve funds to meet future or contingent liabilities or in respect of such other

matters as the Data Commissioner may deem fit; and

(f) any other expenditure for the purposes of this Act.

(3) The annual estimates shall be submitted to the Cabinet Secretary for tabling in the National Assembly.

Accounts and Audit.

69. The annual accounts of the Office shall be prepared, audited and reported in accordance with the provisions of Articles 226 and 229 of the Constitution, the Public Finance Management Act, 2012, or any other law relating to audit of public entities.

No. 18 of 2012.

Annual reports.

70. (1) The Data Commissioner shall, within three months after the end of each financial year, prepare and submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year.

(2) The Cabinet Secretary shall submit the annual report before the National Assembly within three months of receipt of the report under subsection (1).

(3) The annual report shall contain in respect of the year to which it relates—

(a) the financial statements and description of activities of the Office;

(b) such other statistical information as the Data Commissioner may consider appropriate relating to the Data Commissioner's functions;

(c) the impact of the exercise of any of Data Commissioner's mandate or function;

(d) any impediments to the achievements of the object and purpose of this Act or any written law; and

(e) any other information relating to its functions that the Data Commissioner may consider necessary.

PART X—PROVISIONS ON DELEGATED POWERS

Regulations.

71. The Cabinet Secretary may, make regulations generally for giving effect to this Act, and for prescribing anything required or necessary to be prescribed by or under this Act.

(2) Without prejudice to the generality of subsection (1), regulations made under that subsection may provide for—

(a) the requirements which are imposed on a data controller or data processor when processing personal data;

(b) mechanisms of conducting certification program;

(c) the contents which a notice or registration by a data controller or data processor should contain;

(d) information to be provided to a data subject and how such information shall be provided;

(e) the levying of fees and taking of charges;

(f) the measures to safeguard a data subject's rights, freedoms and legitimate interests;

(g) the processing of data through a data server or data centre in Kenya;

(h) issuing and approval of codes of practice and guidelines; or

(i) any other matter that the Cabinet Secretary may deem fit.

(3) For the purposes of Article 94(6) of the Constitution—

(a) the purpose and objective of the delegation under this section is to enable the Cabinet Secretary to make regulations for better carrying into effect the provisions of this Act;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and fulfilment of the objectives specified under this section.

(4) The principles and standards applicable to the delegated power referred to under this Act are those found in—

(a) the Statutory Instruments Act, 2013;

(b) the Interpretation and General Provisions Act;

(c) the general rules of international law as specified under Article 2(5) of the Constitution; and No. 23 of 2013.

(d) any treaty and convention ratified by Kenya under Article 2(6) of the Constitution. Cap 2.

PART XI—MISCELLANEOUS PROVISIONS

Offences of unlawful disclosure of personal data.

72. (1) A data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected commits an offence.

(2) A data processor who, without lawful excuse, discloses personal data processed by the data processor without the prior authority of the data controller commits an offence.

(3) Subject to subsection (4), a person who—

(a) obtains access to personal data, or obtains any information constituting such data, without prior authority of the data controller or data processor by whom the data is kept; or

(b) discloses personal data to third party, commit an offence.

(4) Subsection (3) shall not apply to a person who is an employee or agent of a data controller or data processor acting within the scope of such mandate.

(5) A person who offers to sell personal data where such personal data has been obtained in breach of sub-section (1) commits an offence

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

General penalty.

73. (1) A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.

(2) In addition to any penalty referred to in sub-section (1), the Court may—

(a) order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence; or

(b) order or prohibit the doing of any act to stop a continuing contravention.

Codes, guidelines and certification.

74. (1) The Data Commissioner may, for the purpose of this Act—

(a) issue guidelines or codes of practice for the data controllers, data processors and data protection officers;

(b) offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with this Act;

(c) require certification or adherence to code of practice by a third party;

(d) develop sector specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education, social Protection and any other area as the Data Commissioner may determine.

(2) A certification issued under this section shall not alter the responsibility of the data controller or data processor for compliance with this Act.

Consequential amendments.

75. The laws specified under the Second Schedule are amended in the manner specified.

FIRST SCHEDULE (s.15)

I,.....……, make oath/solemnly affirm/declare that I will faithfully and honestly fulfil my duties as the Data Commissioner in conformity with the Data Protection Act and that I shall not, without the due authority in that behalf, disclose or make known any matter or thing which comes to my knowledge by reason of discharge of my duties.

……

Magistrate/Judge

SECOND SCHEDULE (s.75)

CONSEQUENTIAL AMENDMENTS

Written Law	Provision	Amendment
Births and Deaths Act (*Cap*. 149)	s.7	Add the following new sub-section immediately after subsection (3)— (4) The Register shall be maintained in accordance with the principles of data protection set out in the Data Protection Act.
Capital Markets Act (*Cap*. 485A)	s.11(3)	Insert the following new paragraph immediately after paragraph (v)— (va) ensure processing of personal data in the operations of capital markets is in accordance with principles set out under the Data Protection Act, 2018.
	Insertion of new section	Insert the following new section immediately after section 13B—
	Data protection principles.	**13C.** The principles of personal data protection as set out in the Data Protection Act shall apply to the collection and processing of personal data by the Authority or any person authorized by the Authority.
	18C (2)	Insert the following new paragraph immediately after paragraph (d) — (e) mechanisms of protecting personal data of the data subjects in compliance with the Data Protection Act.
Independent Electoral and Boundaries Commission Act.	s.25	Adding the following new paragraph immediately after paragraph (h) — (i) the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters under this Act.

	s.27	Adding the following new subsection immediately after subsection (5) — (6) The Commission shall ensure the management of personal data is in accordance with the principles of personal data protection as set out in the Data Protection Act.
Kenya National Examinations Council Act	s.10(2)	Insert the following new paragraph immediately after paragraph (m)— (n) to align its Regulations on the collection and processing of information which consists of personal data with the Data Protection Act.
Employment Act, 2007.	s.61	Adding the following new subsection— (2) Where an employer maintains such a register, the register shall be maintained in accordance with the principles of data protection as set out in the Data Protection Act.
The Kenya Citizenship and Immigration Act, 2011.	Insertion of new section	Insert the following new section immediately after section 3— Personal data of individuals. 3A. Personal data of individuals obtained under this Act shall be held and maintained in accordance with the principles of data protection set out in the Data Protection Act.
Basic Education Act, 2013.	s.79	Add the following new sub-section immediately after sub-section (2)— (3) The Board shall deal with any relevant personal data collected and so held in the register according to the data principles set out in the Data Protection Act.
Universities Act, 2012.	s. 13	Add the following new sub-section immediately after sub-section (3) —

(3A) Any information containing personal data presented to the Commission shall be handled in accordance with data protection principles set out in the Data Protection Act.

The Central Depositories Act, 2000.	s.36 (6)	Insert the following new sub-section immediately after sub-section (6) —
		(7) A record of depositors required by an issuer under sub-section (1) shall be issued and maintained in accordance with the principles of data protection set out in the Data Protection Act, 2019.
	S.47	Insert the following new sub-section immediately after sub-section (1)—
		(2) The disclosure of information under this Act shall be done according to the data principles set out in the Data Protection Act, 2019.
Anti-Money Laundering and Proceeds of Crime Act, 2009.	s.40	Insert the following new sub-section immediately after sub-section (1)—
		(2) The sharing of information by the Centre shall be with adherence to the data principles set out in the Data Protection Act, 2019.
	s.13	Insert the following new sub-section immediately after sub-section (1)—
		(2) the information collected on natural persons under this section shall be dealt according to the data principles set out in the Data Protection Act, 2019.
Kenya Information and Communications Act, 1998.	s.23 (2)	Insert the following new paragraph immediately after paragraph (e)—
		(ee) ensure processing of personal data of subscribers is in accordance with principles set out under the Data Protection Act, 2019.
	s.25 (3)	Insert the following new paragraph immediately after paragraph (c)—
		(cc) to ensure necessary steps are taken to secure the integrity of personal data under their possession or

control through the adoption of appropriate, reasonable, technical and organizational measures to prevent the loss of, damage to or unauthorized destruction and prevent any unlawful access to or unauthorized processing of personal data.

Insolvency Act, 2015. s. 148 Insert the following new section immediately after section 148—

148A. The principles of personal data protection set out in the Data protection Act 2018 shall apply with necessary modifications to the processing and handling, by the bankruptcy trustee, of *the bankrupt's* personal data.

I certify that this printed impression is a true copy of the Bill as passed by the National Assembly on Thursday, 7th November, 2019.

Clerk of the National Assembly

Presented for assent in accordance with the provisions of the Constitution of Kenya on the…….at the hour of……

Speaker of the National Assembly

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI