REPUBLIC OF KENYA

PARLIAMENT

SENATE BILLS

(*Bill No. 16 of 2018*)

THE PERSONAL DATA PROTECTION BILL, 2018

(A Bill published in the Kenya *Gazette* Supplement No. 66 of 30th May, 2018 and passed by the Senate, with amendments on Wednesday, 10th July, 2019.)

THE PERSONAL DATA PROTECTION BILL, 2018

ARRANGEMENT OF CLAUSES

Clause

PART VI — MISCELLANEOUS PROVISIONS

THE PERSONAL DATA PROTECTION BILL, 2018

A Bill for

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to promote the protection of personal data; to regulate the manner in which personal data may be processed; to provide persons with rights and remedies to protect their personal data; and to regulate the flow of personal information across the borders of the country; and for connected purposes.

ENACTED by the Parliament of Kenya, as follows—

PART I—PRELIMINARY

Short title.

1. This Act may be cited as the Personal Data Protection Act, 2018 and shall come into operation six months from the date of assent.

Interpretation.

2. In this Act —

"Cabinet Secretary" means the Cabinet Secretary responsible for information and communications;

"Commission" means the Kenya National Commission on Human Rights established by section 3 of the Kenya National Commission on Human Rights Act;

No. 14 of 2011.

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

"Court" means the High Court or any other court with jurisdiction under any law to adjudicate over matters relating to data protection;

"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 the intention that it should be processed

by means of such equipment;

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

(d) where it does not fall under paragraph (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 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;

"disclosure", in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data to another person but does not include a disclosure made directly or indirectly by a data controller or a data processor to its employee or agent for the purpose of enabling the employee or agent to carry out its duties and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller or the data processor, the data shall not be considered as disclosed unless the other information is also disclosed;

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

"personal data" means information relating to an identified or identifiable natural person, including—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education, medical, criminal

or employment history of the person or information relating to financial transactions in which the person has been involved in;

(c) an identifying number, symbol or other particular assigned to the individual;

(d) the biometrics of a person ;

(e) contact details including telephone numbers of the person;

(f) correspondence by a person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence to a third party;

"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;

"processing" means an operation or activity or set of operations by automatic or other means that concerns data or personal data and includes —

(a) collection, organisation, storage, adaptation or alteration of the information or data;

(b) retrieval, consultation or use of the information or data;

(c) disclosure of the information or data by transmission, dissemination or any other means; or

(d) alignment, combination, blocking, deletion or destruction of information or data.

"record" in relation to an agency, means a document or any other source of information compiled, recorded or stored in written form, on film, by electronic process or in any other manner or a record made or kept by a person acting under the authority of law or exercising other official function;

"Secretary" has the meaning assigned to it by section 21 of the Kenya National Commission on Human Rights Act; and

No. 14 of 2011.

"special personal information" means the personal data of a child, biometric data or data revealing a natural person's race, health status or ethnic origin.

Application.

3. (1) This Act shall apply to –

(a) the protection of personal data of a data subject in the processing of such data by –

(i) a data controller or a data processor who is a Kenyan citizen or a legal entity established in the Republic of Kenya; and

(ii) a data controller or a data processor not established in the Republic of Kenya but processes personal data of a data subject who is a resident of the Republic of Kenya; and

(b) the processing by automated or any other means of personal data which forms or is intended to form part of a filing system.

(2) This Act shall not apply to the processing of personal data –

(a) by or on behalf of a public body responsible for matters relating national security the purpose of which is the prevention, detection, investigation or punishment of a crime; or

(b) by a person in the course of a personal or household activity.

(3) Despite the provisions of subsection (2)(a) and except where the security of the country, the life, safety or health of a person, or property is in imminent danger, a public body that intends to process personal data without the consent of the data subject shall make an application *ex parte* to a court for orders to process such data.

PART II – REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Registration of data controllers and data processors.

4. (1) Subject to subsection (2), no person shall act as a data controller or data processor unless registered with the Commission.

(2) The Commission shall prescribe the threshold required

for mandatory registration of a data controller and data processor, and in making such determination, the Commission shall consider –

(a) the nature of industry;

(b) the volumes of data processed;

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

(d) any other criteria the Commission may specify.

Application for registration.

5. (1) A data controller or data processor required to register under section 4 shall apply to the Commission for registration.

(2) An application under subsection (1) shall provide the following particulars –

(a) a description of the personal data to be processed;

(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; and

(f) any other details as may be prescribed by the Commission.

(3) The Commission shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.

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

(5) On receipt of a notification under subsection (4), the Commission shall amend the respective entry in the register.

Duration of the registration certificate.

6. A registration certificate issued under section 5 shall be valid for a period of three years and the holder may apply for the renewal after expiry of the certificate.

Register of data controllers and data processors.

7. (1) The Commission shall keep and maintain a register of registered data controllers and data processors.

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

(3) A person may request the Commission for a certified copy of any entry in the register.

Cancellation or variation of the certificate.

8. The Commission may, on notice, vary terms and conditions of a 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 certificate of registration, without lawful excuse, fails to comply with any requirement of this Act.

Compliance and audit.

9. The Commission 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.

10. (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, scope or 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 perform 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 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 and communicate them to the Commission.

(7) The responsibility of a data protection officer shall be to—

(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;

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

(e) cooperate with the Commission and any other authority on matters relating to data protection.

PART III—OBJECTS AND PRINCIPLES OF PROTECTION OF PERSONAL DATA

Principles of personal data protection.

11. The following principles shall guide the interpretation and application of this Act —

(a) personal data shall —

(i) be collected, processed, stored or dealt with in

any other manner if it is necessary for or directly related to a lawful, explicitly defined purpose and shall not intrude on the privacy of the data subject;

(ii) be collected directly from and with the consent of the data subject;

(iii) only be disclosed to a third party or put to a different use with the consent of the data subject;

(iv) not be kept for a longer period than is necessary for achieving the purpose for which it was collected;

(v) not be processed in a manner that is incompatible with the purpose for which it was collected; and

(vi) shall be accurate, up-to data and complete;

(b) the data subject shall be informed of the purpose to which personal data shall be put and the intended recipients of that data at the time of collection; and

(c) appropriate technical and organizational measures shall be taken to safeguard personal data against the risk of loss, damage, destruction of or unauthorized access to personal information.

Right to protection of privacy.

12. Every person has the right to privacy with respect to their personal data.

Limitation.

13. (1) The right to privacy under Article 31 of the Constitution, with respect to personal data, may be limited for the purpose of safeguarding overriding legitimate interests.

(2) The right to privacy may be limited for purposes of –

(a) prevention, detection, investigation, prosecution or punishment of a crime;

(b) safeguarding rights of the data subject or another person;

(c) public interest; and

(d) compliance with an obligation imposed by law.

Collection of data from data subject.

14. (1) A data controller or data processor shall, subject to subsection (2), where it requires personal data from a data subject, collect such personal data directly from the data subject for a purpose which is specific, explicitly defined and lawful.

(2) A data controller or a data processor shall not be required to collect personal data directly from a data subject where –

(a) the data subject has made the data public ;

(b) the data subject or in the case of a child or a person who is legally incapacitated, the guardian of that child or person, has consented to the collection of personal data from another source;

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

(d) collection of data from another source is necessary-

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

(ii) for the protection of fundamental rights and freedoms of the data subject or another person; or

(iii) to comply with an obligation imposed by law; or

(e) if the life, safety or health of a person or property is in imminent danger.

(3) A data controller or data processor shall collect or process personal data using lawful means and in compliance with the right to privacy and this Act.

Conditions of consent.

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

(2) A data subject may withdraw consent for collection or

processing of personal data at any time.

(3) The withdrawal of consent under sub-section (2) shall not affect the lawfulness of processing of personal data before consent was withdrawn.

Quality of information.

16. (1) A data controller or a data processor that collects or processes personal data shall ensure that the data is complete, accurate, up-to-date and not misleading having regard to the purpose for the collection or processing of the personal data.

(2) Where the data subject is in control of the means of inputting or processing his or her personal data, it shall be the responsibility of the data subject to ensure that personal data is complete, accurate, up-to-date and not misleading.

Rights of a data subject.

17. A data subject has a right to –

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

(b) access their personal data which is in the possession of a data controller or data processor;

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

(d) correction of false or misleading personal data;

(e) the deletion of personal data relating to the data subject which is in possession of a data controller or data processor;

(f) be informed of the period within which personal data is to be stored; and

(g) data portability.

Duty to notify.

18. (1) A data controller or data processor shall, before collecting personal data directly from a data subject, inform the data subject in a language the data subject understands —

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

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

(c) the intended recipient of the personal data;

(d) the name and address of the data controller or

data processor that is collecting the personal data and any other person who may access the collected personal data;

(e) where the information is collected pursuant to any law —

(i) the law requiring or authorising the collection of the information;

(ii) the procedure required to be undertaken in order to comply with the law; and

(iii)whether the giving of the personal data by that data subject is voluntary or mandatory;

(f) the consequences if any, where the data subject fails to provide all or any part of the requested information; and

(g) the right of the data subject specified under section 17 of this Act.

(2) A data controller or a data processor shall not collect personal data from a data subject unless it has taken the steps specified in subsection (1).

(3) Despite subsection (2), where—

(a) it is not practicable for a data controller or a data processor to comply with subsection (1) before collecting information; or

(b) the whereabouts of the data subject are not known,

the data controller or the data processor shall, as soon as practicable after the information is collected, comply with the provisions of subsection (1).

When not to notify.

19. (1) A data controller or data processor shall not be required to take the steps specified under section 17 if the data controller or the data processor has, prior to collecting the personal data, taken those steps within the past twelve months when collecting the same personal data or personal data of the same kind from that data subject.

(2) Where a data controller or data processor collects personal data under subsection (1) to be used for a different purpose from the one for which the personal data was first collected or where the circumstances of the data subject have

changed, the data controller or data processor shall notify the data subject of the new use to which the personal data shall be put to.

(3) A data controller or data processor shall notify a data subject that a waiver of his or her rights under this Act shall be construed as consent and authorisation for the data controller or a data processor to collect the information.

Lawfulness of processing personal data.

20. (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;

(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 data controller or a data processor is subject;

(iii) in order to protect the fundamental rights and freedom of the data subject or another person;

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

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

(vi) for the protection of legitimate interests pursued by a data controller or data processor having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject;

(vii) for the purpose of historical, statistical or scientific research; or

(viii) for such other purpose as the Cabinet Secretary may prescribe.

(2) Further processing of personal data shall be in accordance

with the purpose for which the personal data was collected.

Automated processing.

21. (1) A data subject shall not be subject to a decision that is based solely on automated processing of personal data which produces legal effect concerning the data subject or which significantly affect the data subject without human intervention.

(2) Subsection (1) shall not apply to a data subject where the decision is –

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

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

(c) based on the explicit consent of the data subject.

(3) Where a data controller or data processor intends to make a decision based on automated processing and which produces a legal effect or significantly affects the data subject, the data subject shall have the right to –

(a) be notified in writing before a decision is taken;

(b) be provided with an explanation of the reason for and the consequences of the decision; and

(c) raise an objection against a decision made under this section to the data controller or data processor for the protection of the data subject's legitimate interests.

(4) The data controller or data processor shall consider the issues under subsection (3)(c) and notify the data subject of its findings and decision within seven days of receipt of the objection.

Data processing.

22. (1) A data controller or a data processor that processes personal data shall ensure that the data is processed –

(a) without infringing the right to privacy of the data subject or another person;

(b) in a lawful manner; and

(c) in a reasonable manner.

(2) Whenever personal data concerning a data subject is to be processed, the data subject shall have the right, upon request, to—

(a) information relating to the person processing the data;

(b) information on the place of origin of the data;

(c) information on the use to which the data collected will be put to;

(d) information relating to any other person to whom the data is to be disclosed;

(e) the rectification of incorrect data; and

(f) the deletion of data which has been processed without the consent of the data subject.

Protection and security of personal data.

23. (1) A data controller or a data processor shall take the necessary steps to ensure the integrity of personal data in its possession or control through the adoption of appropriate and reasonable technical and organisational measures to prevent —

(a) loss, damage or unauthorised destruction; and

(b) unlawful access to or an unauthorised processing.

(2) In compliance with subsection (1), a data controller or data processor shall take reasonable measures to –

(a) identify reasonably foreseeable internal and external risks;

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

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated.

(3) In implementing the measures under subsection (2), a data controller or data processor shall take into account –

(a) the amount of personal data processed;

(b) the nature of personal data being processed;

(c) the extent of the processing of the personal data;

(d) special risks that exist in the processing of the personal data;

(e) the period of retention of the personal data; and

(f) the ease of accessibility.

(4) A data controller or a data processor shall observe generally acceptable security practices and procedures, including specific industry or professional rules and regulations.

Notification of security compromises.

24. (1) Where there is a breach of security or there are reasonable grounds to believe that personal data has been accessed or processed contrary to this Act, a data controller or data processor shall –

(a) within seventy two hours after the discovery of the unauthorised access or processing of the data, notify the Commission and the data subject; and

(b) take steps to ensure the restoration of the integrity of the information system.

(2) The notification under subsection (1)(a) shall set out sufficient information to enable the data subject to take protective measures against potential consequences of the data breach, including —

(a) description of the nature of the breach;

(b) description of the likely consequences of the breach;

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

(d) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the breach; and

(e) where possible, the identity of the person who may have accessed or processed the personal data.

(3) A data controller or data processor may delay notification to the data subject under subsection (1)(a) for the purpose of preventing, detecting or investigating a crime by the relevant

public entity.

(4) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller within forty-eight hours of becoming aware of such breach.

Data protection impact assessment.

25. (1) Where processing of personal data is likely to result in high risk to the rights and freedoms of a data subject due to the nature, scope, context or purpose, a data controller or data processor shall, prior to processing, carry out an impact assessment.

(2) The impact assessment shall include –

(a) a systematic description of the intended personal data processing operations and the purpose for processing;

(b) an assessment of the necessity and proportionality of personal data processing operations taking into account the purposes for processing of personal data;

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

(d) the measures envisaged to address the risks, including 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 interested persons.

(3) Where an impact assessment indicate that the processing of personal data would result in high risk to the rights and freedoms of a data subject, a data controller or data processor shall consult the Commission prior to processing personal data.

(4) The Commission shall set out the guidelines for carrying out an impact assessment under this section.

Access to personal data.

26. (1) Where a data controller or data processor is in possession of personal data or where a person believes that a data controller or data processor is in possession of personal data relating to him or her, that person —

(a) may obtain from the data controller or data processor a confirmation as to whether the agency possesses such

personal data and the purposes for processing the personal data; and

(b) shall have access to that data.

(2) A data controller or data processor to which an application for access to personal data has been made may charge a prescribed fee for the provision of the personal data and the fee shall not exceed the actual costs of making copies of such information and if applicable, supplying them to the data subject.

(3) The procedure for making an application for, and obtaining access to information under the Access to Information Act shall apply to subsection (1).

No. 31 of 2016.

Correction of information.

27. (1) A data controller or data processor which holds personal data shall, if requested by a data subject or on its own initiative, take steps to correct or delete false or misleading data.

(2) A data subject may, pursuant to Article 35 (2) of the Constitution, request a data controller or a data processor which is in possession or control personal data relating to the data subject to correct, delete or destroy false, misleading, outdated or such other personal data relating to the data subject as the data subject may request.

(3) A request made under subsection (2) shall –

(a) be in writing;

(b) specify the information to be corrected or deleted; and

(c) in the case of a request for correction, specify the manner in which such information should be corrected.

(4) The agency shall consider the request and inform the data subject of the decision within seven days of the receipt of the request.

(5) Where an agency rejects a request under subsection (2), it shall inform the data subject of the rejection and the reasons for the rejection in writing.

(6) Where a data controller or data processor approves a request under subsection (2), the data controller or data processor shall –

(a) correct or delete the data within seven days of approval of the request;

(b) inform the data subject of the action taken within seven days of taking the action under paragraph (a); and

(c) where the data had been shared with any other person, inform that other person of the action taken and require that person to correct or delete the data.

(7) A data controller or data processor shall not correct or delete personal data which is the subject of a case before a court.

Right to data portability.

28. (1) A data subject has the right to receive personal data which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit the data obtained under subsection (1) to another data controller or data processor.

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

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

(a) processing is 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 another.

(5) An data controller or data processor shall comply with data portability requests, free of charge and within a period of seven days from the date of the request or as may be determined by the Commission where personal data is numerous or complex.

Retention of information.

29. (1) A data controller or data controller that collects or processes personal data shall not keep the data for a longer period than is provided under any law or necessary to achieve the purposes for which the data was collected or processed, unless –

(a) the data subject consents to the retention;

(b) the retention of the data is authorised by law;

(c) the retention of the data is necessary for a lawful purpose related to the function or activity performed by the data controller or the data processor;

(d) the retention of the data is required by virtue of a contract between the data subject and the data controller or the data processor; or the retention is for historical, statistical, journalistic literature and art or research purposes; or

(e) the retention is for historical, statistical, journalistic literature and art or research purposes.

(2) A data controller or data processor that retains data for historical, statistics or research purposes shall ensure that personal data is protected against access or use for unauthorised purposes.

(3) A data controller or data processor may, for purposes of subsection (2), anonymise or pseudonymise the data retained under subsection (1) in such a manner as to ensure that the data subject is no longer identifiable.

(4) A data controller or data processor shall, at the expiry of the retention period, destroy or delete personal data in a manner that prevents its deconstruction in an intelligible form.

Commercial use of data.

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

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

(b) it is authorised to do so under any other 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 Commission may prescribe practice guidelines for commercial use of personal data in accordance with this Act.

Use of unique identifiers.

31. (1) A data controller or data processor that assigns unique identifiers to persons shall take all reasonable steps to ensure that

unique identifiers are assigned only to persons whose identity is clearly established.

(2) A data controller or data processor shall not require a person to disclose any unique identifier assigned to him or her unless the disclosure is for one of the purposes for which that unique identifier was assigned or for a connected purpose.

PART IV- PROCESSING OF SPECIAL INFORMATION

Prohibition on processing of special information.

32. (1) A data controller or data processor shall not process special personal data

(2) The provisions of subsection (1) shall not apply where processing of personal data is –

(a) carried out with the consent of the data subject or in the case of a data subject who is a child or a person who is legally incapacitated, the guardian;

(b) required under national or international law;

(c) for the purpose of statistical or research purposes;

(d) with respect to information that has been made public by the data subject; or

(e) necessary for the establishment, exercise or defence of a legal claim.

Data subject's race or ethnic origin.

33. A data controller or data processor may process personal data relating to a data subject's race or ethnic origin if the processing is-

(a) essential for the identification of the data subject; and

(b) in compliance with lawful measures for the protection and advancement of a category of persons disadvantaged by unfair discrimination.

Data subject's health.

34. A data controller or data processor may process personal data relating to a data subject's health where the data controller or the data processor is-

(a) a medical institution processing information for purposes of treatment and care of the data subject;

(b) an insurance company or a medical scheme processing information for purposes of entering into

or performing an insurance contract;

(c) a school processing the information for purposes of providing special support for students in connection with their health;

(d) a public or private body acting under a lawful duty to manage the welfare of a data subject; or

(e) an administrative body, pension fund, or employer processing information for purposes of implementation of the law relating to the health of the data subject.

Personal data of children.

35. (1) A data controller or data processor shall not process personal data of a child unless the processing is-

(a) carried out with the prior consent of the parent or guardian of the child;

(b) necessary to comply with the law;

(c) for research or statistical purposes; or

(d) in the best interest of the child.

(2) A data controller or data processor shall adopt appropriate measures for age verification and the giving of consent for processing of personal data.

Transborder flow of personal data.

36. (1) A data controller or data processor shall not transfer personal data of a data subject outside the territory of the Republic of Kenya unless-

(a) the Commission is satisfied that the other country is subject to a law or agreement that requires the putting in place of adequate measures for the protection of personal data;

(b) the data subject consents to the transfer; and

(c) the transfer is necessary -

(i) for the performance or conclusion of a contract between the data subject and the data processor or data controller;

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

(iii) for the protection of fundamental rights and freedoms of a person; or

(iv) in the interest of the public.

(2) The Cabinet Secretary in consultation with the Commission shall prescribe guidelines for the transfer of personal data outside the country and the filing of reports on personal data transferred outside the country by a data controller or data processor.

Safeguards for special personal data.

37. (1) A data controller or data processor shall, for the purposes of this Part, adopt appropriate measures to ensure that the data subject is not identifiable including anonymising or pseudonymising the data used for statistical or research purposes.

(2) The Cabinet Secretary in consultation with Commission may provide additional guidelines on protection of special personal data.

PART V – OVERSIGHT AND ENFORCEMENT

Role of the Commission.

38. The Commission shall oversee the implementation of and be responsible for the enforcement of this Act.

Functions of the Commission.

39. (1) The functions of the Commission shall be to—

(a) promote the protection and observance of the right to privacy;

(b) monitor, investigate and report on the observance of the right to privacy;

(c) formulate, implement and oversee programmes intended to raise public awareness of the right to privacy and obligations;

(d) receive and investigate any complaint relating to infringement of the rights of a person under this Act;

(e) provide a framework or mechanism for the effective management of conflicts and the resolution of disputes under this Act; and

(f) perform such other functions as may be prescribed by any other law or as the Commission may consider necessary for the promotion and protection of human

rights.

(2) The Commission shall, in performing its functions under this Act—

(a) be guided by the national values and principles of governance under Article 10 of the Constitution;

(b) have regard to the applicable international information management and dissemination standards relating to data protection;

(c) ensure that data controllers and data processors have put in place adequate safeguards for the protection of personal data;

(d) take statements under oath in relation to any investigation it is undertaking; and

(e) take such action as may be necessary for the performance of its functions under this Act.

(3) The Commission shall have all the powers necessary for the performance of its functions under this Act.

Inquiry into complaints.

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

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

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

(4) A complaint lodged under subsection (1) shall contain such particulars as the Commission may prescribe.

(5) The Commission may, upon receipt of a complaint under subsection (1) —

(a) require the relevant data controller or data processor to respond to the complaint within such time as may be specified by the Commission;

(b) request for such further information from the

complainant as it may consider necessary from the complainant; or

(c) initiate such inquiry as it considers necessary, having regard to the nature of the complaint.

(6) Where a data controller or a data processor fails respond within the time stipulated by the Commission under subsection (5)(a), the Commission may proceed to inquire into the complaint.

(7) Where, upon receipt of the response from the agency under subsection (5), the Commission is satisfied that no further action is required or that the required action has been initiated by that data controller or the data processor, the Commission shall, in writing, inform the complainant accordingly and take no further action.

(8) Despite subsection (1), the Commission may, on its own initiative, commence an investigation under this Act.

Discretion not to take action on a complaint.

41.(1) The Commission may, upon receipt of a complaint under section 40(1), decline to take action or further action as the circumstances may require, if, in the opinion of the Commission—

(a) the length of time that has elapsed between the date when the cause of action arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(b) the complaint is trivial, frivolous or vexatious or is not made in good faith;

(c) the complainant does not desire that action be taken or, as the case may be, continued;

(d) the complainant does not have a personal interest in the subject matter of the complaint;

(e) there is in force, a code of practice that provides a procedure that would adequately address the complaint and the complainant has failed to pursue this avenue of redress; or

(f) there is in existence an adequate remedy or other right of appeal other than to the Commission, that it would be reasonable for the complainant to pursue.

(2) The Commission may decline to take further action on a complaint if, in the course of investigating the complaint, it

appears to the Commission that having regard to all the circumstances of the case, no further action is necessary.

(3) Where the Commission declines to take action or further action on a complaint, it shall inform the complainant of its decision and the reasons for its decision.

Settlement of complaints.

42. (1) Where it appears to the Commission that it may be possible to secure a settlement with respect to a complaint between any of the parties concerned and, if appropriate, a satisfactory assurance against the doing or repetition of any action or similar action of the kind that forms the basis of the complaint by the person concerned, the Commission may, without investigating the complaint or undertaking further investigations as the case may be, secure such settlement or assurance.

(2) Where, upon inquiry into a complaint lodged under section 40(1) the Commission is satisfied that a person has contravened, is contravening or may contravene any of the provisions of this Act, the Commission may issue a notice to that person requiring the person to take or refrain from taking, within such period as may be specified, such action as the Commission may specify.

(3) The Commission may, pursuant to subsection (2), require a person to rectify, block, erase or destroy any inaccurate data.

(4) Despite the provisions of this Act, a person whose personal data is collected or processed contrary to this Act or who suffers loss as a result of disclosure of personal data may lodge a claim before a court for an appropriate remedy.

(5) In determining a claim under subsection (4) a court shall consider –

(a) the nature and the seriousness of the breach;

(b) the categories of personal data affected;

(c) any benefit gained or loss suffered as a result of the breach;

(d) the number of previous violations;

(e) the duration of time over which the breach occurred;

(f) any action taken by the data controller or data processor to remedy or mitigate the breach; and

(g) the nature and status of the data controller or data

processor.

PART VI – MISCELLANEOUS PROVISIONS

Protection against certain actions.

43. (1) Where a data controller or a data processor discloses personal data in good faith pursuant to this Act —

(a) no civil or criminal proceedings shall lie against the data controller or the data processor in respect of disclosing the data, or for any consequences that may arise as a result of disclosing the data; and

(b) no civil or criminal proceedings shall lie in respect of any publication of the disclosed data against the author of the data or any other person by reason of that author or other person having supplied the data to a data controller or a data processor.

(2) The disclosure of or giving of access to a person of any personal data pursuant to a request made under section 25 shall not be construed, for the purposes of the law relating to defamation or breach of confidence or infringement of copyright, to constitute an authorisation or approval of the publication of the information by the person to whom the information is disclosed or access is given.

Offences.

44. (1) A person who collects or processes personal data in any manner contrary to the provisions of this Act commits an offence and is liable, on conviction, to a fine not exceeding one million shillings or to a term of imprisonment not exceeding five years, or to both.

(2) Despite subsection (1), where the offence –

(a) committed relates to special personal information the person shall be liable, on conviction, to a fine not exceeding five million shillings or to a term of imprisonment not exceeding ten years; or

(b) is committed by a body corporate, the body corporate shall be liable, on conviction, to a fine not exceeding three million shillings or two percent of its annual turnover, whichever is higher.

(3) A person who —

(a) without reasonable excuse, obstructs, hinders or prevents the Commission or any other person from the

performance of their functions or the exercise of their powers under this Act;

(b) makes any statement or gives any information to the Commission or any other person exercising powers under this Act, knowing the statement or information to be false or misleading;

(c) holds himself or herself out as having authority to perform any action or exercise any powers under this Act when he or she does not hold that authority; or

(d) without reasonable cause, fails to comply with any notice issued under this Act,

commits an offence and is liable, on conviction, to a fine not exceeding one hundred thousand shillings or to a term of imprisonment not exceeding two years, or to both.

(4) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributed to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, that person as well as the body corporate shall be guilty of that offence.

(5) In addition to any penalty prescribed under this section, a Court may make orders –

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

(b) prohibiting the doing of any act to stop continuing commission of an offence.

Regulations.

45. (1)The Cabinet Secretary may, in consultation with the Commission, make regulations prescribing anything required by this Act to be prescribed or generally for the better carrying out of the provisions of this Act.

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

(a) the making of an application under this Act;

(b) the form in which information requested under this

Act is to be supplied;

(c) the procedure for the service of notices and documents under this Act; or

(d) forms such as may be necessary to give full effect to the implementation or administration of this Act.

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

(a) the authority of the Cabinet Secretary to make regulations shall be limited to bringing into effect the provisions of this Act and the fulfilment of the objectives specified under subsection (1); and

(b) the principles and standards set out under the Interpretation and General Provisions Act and the Statutory Instruments Act, 2013 in relation to subsidiary legislation shall apply to regulations made under this Act.

Cap. 2.
No. 23 of 2013.

Codes, guidelines and certifications.

46. The Commission may –

(a) issue guidelines or codes of practice;

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

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

(d) develop sector specific guidelines as the Commission may determine.

I certify that this printed impression is a true copy of the Bill as passed by the Senate on Wednesday, 10th July, 2019.

Clerk of the Senate

Endorsed for presentation to the National Assembly in accordance with the provisions of standing order 156 of the Senate Standing Orders.

Speaker of the Senate