NATIONAL COUNCIL FOR
LAW REPORTING
LIBRARY

SPECIAL ISSUE

Kenya Gazette Supplement No. 66 (Senate Bills No. 16)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

SENATE BILLS, 2018

NAIROBI, 30th May, 2018

CONTENT

Bill for Introduction into the Senate—

NATIONAL COUNCIL FOR LAW REPORTING
RECEIVED
02 JUL 2018
P.O. Box 10443-00100
NAIROBI, KENYA
TEL: 2719231 FAX: 2712004

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

RECEIVED

THE DATA PROTECTION BILL, 2018

ARRANGEMENT OF CLAUSES

Clause

PART I—PRELIMINARY

PART II—OBJECTS AND PRINCIPLES OF PROTECTION OF PERSONAL DATA

PART III—PROCESSING OF SPECIAL INFORMATION

PART IV—OVERSIGHT AND ENFORCEMENT

PART V—MISCELLANEOUS PROVISIONS

THE 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 Data Protection Act, 2018.

Interpretation.

2. In this Act —

"agency" means a person who collects or processes personal data;

"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.

"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 person who, either alone or together with other persons, controls the contents and use of personal information;

"data subject" means a person from whom personal data is obtained;

"disclosure", in relation to personal information, includes the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his 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, the data shall not be considered as disclosed unless the other information is also disclosed;

"exempt information" means information that may be withheld by a public entity or a private body in accordance with section 6 of the Access to Information Act; No. 31 of 2016.

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

"personal data" means information about a 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; No. 14 of 2011.

(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 fingerprints or blood type of the 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;

(g) a person's views or opinions about another person ; and

(h) any information given in support or in relation to a grant, award or prize proposed to be made to a person;

"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, 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

"special personal information" means –

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or biometric information of a data subject; or

(b) any information about a data subject relating to the alleged commission of an offence or any proceedings in respect of any offence allegedly committed by a data subject.

Application.

3. This Act does not apply to the processing of personal data by or on behalf of a public body-

(a) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorism and related activities, defence or public safety; or

(b) the purpose of which is the prevention, detection and identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, prosecution of offenders or the execution of sentences or security measures.

PART II—OBJECTS AND PRINCIPLES OF PROTECTION OF PERSONAL DATA

Principles of data protection.

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

(a) information shall 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;

(b) information shall be collected directly from and with the consent of the data subject;

(c) where information relating to the data subject is held by a third party, the information may only be released to another person or put to a different use with the consent of the data subject;

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

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

(f) information shall not be distributed in a manner that is incompatible with the purpose for which it was collected with the consent of the person and subject to any notification that would attract objection;

(g) reasonable steps shall be taken to ensure that the information processed is accurate, up-to date and complete;

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

(i) data subjects have a right of access to their personal information and a right to demand correction if such information is inaccurate.

Right to protection of privacy.

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

Limitation.

6. (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) national security;

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

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

(d) public interest; and

(e) compliance with an obligation imposed by law.

Collection of data from data subject.

7. (1) An agency shall, subject to subsection (2), where it requires personal data from a person, collect such information directly from the data subject for a purpose which is specific, explicitly defined and lawful.

(2) An agency shall not be required to collect personal data directly from a data subject where –

(a) the data is a matter of public record;

(b) the data subject or a competent person, where the data subject is a child, has consented to the collection from another source;

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

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

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

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

(ii) for the protection of the interests of the data subject or another person;

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

(iv)in the interest of national security; or

(f) compliance is not reasonably practical in the circumstances of the case.

(3) An agency shall collect, store or use personal data—

(a) using lawful means; or

(b) using means that, in the circumstances, do not intrude to an unreasonable extent, upon the personal affairs of the data subject except in accordance with this Act or any other written law.

Quality of information.

8. An agency 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.

Rights of a data subject.

9. A data subject has a right to –

(a) be informed by the agency of the use to which the data is to be put;

(b) access the data with respect to the data subject which is in possession of an agency;

(c) object to the collection or processing of all or part of data by an agency;

(d) correction of false or misleading data;

(e) deletion of misleading, false or data which has been objected to; and

(f) an explanation in respect of the processing of data and the outcome of such processing;

Duty to notify.

10. (1) Before an agency collects personal data directly from a data subject, the agency shall in so far as is reasonably practicable, inform the data subject —

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected and specify the use to which such information shall be put;

(c) the intended recipient of the information;

(d) the name and address of the agency that is collecting the information, the agency that will hold the information and whether or not any other agency will receive the information;

(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 supply of the information by that data subject is voluntary or mandatory;

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

(h) the right of access to, and correction of, personal data provided under section 13 and 15 of this Act.

(2) An agency 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 an agency to comply with subsection (1) before collecting information; or

(b) the whereabouts of the data subject are not known, the agency shall, as soon as practicable after the information is collected, comply with the provisions of subsection (1).

When agency may not notify.

11. (1) An agency shall not be required to take the steps specified under section 10 if that agency has, prior to collecting the information, taken those steps in the recent past when collecting the same information or information of the same kind from that data subject.

(2) Where an agency collects information under subsection (1) to be used for a different purpose from the one for which the information was first collected or where the circumstances of the data subject has changed, the agency shall notify the data subject of the use to which the information shall be put to.

(3) An agency 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 agency to collect the information.

Exemptions.

12. An agency shall not be deemed to have collected personal data contrary to the provisions of section 7 to 11 if -

(a) the information is publicly available;

(b) the data subject authorised the collection of the data from a third party;

(c) non-compliance does not prejudice the interests of the data subject;

(d) non-compliance is necessary—

(i) to avoid a threat to the maintenance of law and order by any public entity, including the prevention, detection, investigation, prosecution and punishment of an offence;

(ii) for the enforcement of a law imposing a pecuniary penalty;

(iii) for the protection of public revenue and property;

(iv) for the institution of proceedings or the conduct of proceedings that have been instituted before any Court, tribunal or the Commission; or

(v) for the purpose of an exemption as set out in the law relating to access to information;

(e) compliance would prejudice the purposes for which the information is collected;

(f) compliance is not reasonably practicable in the circumstances of the particular case;

(g) the information—

(i) was not to be used in a manner which resulted in the identification of the data subject; or

(ii) was used for statistical or research purposes and shall not be published in a form that could reasonably be expected to result in the identification of the data subject.

(h) the information is collected pursuant to an authority granted under this Act or any other written law.

Prohibition of profiling.

13. (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) An agency shall not be deemed to have profiled a data subject if the processing of data was necessary to avoid a threat to the maintenance of law and order by any public entity, including the prevention, detection, investigation, prosecution and punishment of a crime.

Data processing.

14. (1) An agency 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) the place of origin of the data;

(c) 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 transmitted;

(e) the rectification of incorrect data; and

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

Protection and security of personal data.

15. (1) An agency shall take the necessary steps to ensure the integrity of personal data in its possession or control through the adoption of appropriate, 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), an agency 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) An agency shall observe generally acceptable security practices and procedure, including specific industry or professional rules and regulations.

Notification of security compromises.

16. Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or processed by unauthorised person, the agency shall –

(a) as soon as reasonably practicable 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.

Access to personal data.

17. (1) Where an agency stores personal data or where a person believes that an agency is storing personal data relating to him or her, in a readily retrievable form, the person—

(a) may obtain from the agency, a confirmation as to whether the agency holds such personal data; and No. 31 of 2016.

(b) shall have access to that data.

(2) Subsection (1) shall not apply to exempt information.

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

Correction of information.

18. (1) An agency 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 an agency that holds personal data relating to the data subject to correct, delete or destroy false or misleading data.

(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) An agency may reject a request under subsection (2) on the basis that the request does not amount to a request for the correction or deletion of data.

(7) Where an agency determines to correct or delete the data, it shall do so within a period of seven days and inform the data subject of the action taken within a period of seven days from the date of the action.

Retention of information.

19. (1) An agency 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 reasonably necessary for a lawful purpose related to a function or activity or

(d) the retention of the data is required by virtue of a contract between the parties to the contract.

(2) Subsection (1) shall not apply to personal data retained for purposes of –

(a) history;

(b) statistical; or

(c) research.

(3) Agency that retains data for historical, statistics or research purposes shall ensure that personal data is protected against access or use for unauthorised purposes.

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

Misuse of information.

20. Subject to this Act or any other written law, an agency that holds personal data that was obtained in connection with one purpose shall not use the data for any other purpose.

Commercial use of data.

21. 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.

Use of unique identifiers.

22. (1) An agency 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) An agency 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.

Interference with personal data.

23. A person who interferes with personal data of a data subject or infringes on the right of a person to privacy commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand shillings or to imprisonment for a term not exceeding two years, or to both.

PART III—PROCESSING OF SPECIAL INFORMATION

Prohibition on processing of special

24. (1) An agency shall not process special personal information.

information.

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

(a) carried out with the consent of the data subject;

(b) required under national or international law;

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

(d) publicly available.

Processing of information concerning religious or philosophical beliefs.

25. An agency may process information relating to the religious or philosophical beliefs of a data subject where the agency is a spiritual or religious organisation or an independent section of a spiritual or religious organisation and where the data subject –

(a) is an employee or member of that organisation; and

(b) has consented to the processing of that information.

Data subject's race or ethnic origin.

26. An agency may process personal information relating to a data subject's race or ethnic origin if the processing is-

(a) essential to 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 trade union activities.

27. An agency may process personal information relating to a data subject's trade union membership where-

(a) the agency is a trade union to which the data subject belongs; and

(b) the processing is necessary for the aims of the trade union.

Data subject's health.

28. An agency may process personal information relating to a data subject's health where the agency is-

(a) a medical institution or social service 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.

29. An agency shall not process personal data of a child unless the processing is-

(a) carried out with the prior consent of the parent or guardian or any other person having the authority to make decisions on behalf of the child;

(b) necessary to comply with the law;

(c) for research or statistical purposes; or

(d) publicly available.

Data subject's political persuasion.

No. 11 of 2011.

30. An agency may process personal information concerning a data subject's political persuasion if the agency is a political party formed under the Political Parties Act or public entity whose functions are political in nature and the personal information-

(a) relates to the members of the agency; and

(b) is necessary to the formation or carrying out of the activities of the agency.

Transborder flow of personal data.

31. An agency shall not transfer personal data of a data subject outside the territory of the Republic of Kenya unless-

(a) the third party 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;

(c) the transfer is necessary for the performance or conclusion of a contract between the agency and the third party; and

(d) the transfer is for the benefit of the data subject.

PART IV—OVERSIGHT AND ENFORCEMENT

Role of the Commission.

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

Functions of the Commission.

33. (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 agencies 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.

34. (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 agency 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 an agency 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 agency, 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.

35. (1) The Commission may, upon receipt of a complaint under section 34(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.

36. (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 34(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 persons may lodge a claim before the Court for an appropriate remedy.

PART V—MISCELLANEOUS PROVISIONS

Protection against certain actions.

37. (1) Where an agency discloses personal data in good faith pursuant to this Act —

(a) no civil or criminal proceedings shall lie against the agency 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 an agency.

(2) The disclosure of or giving of access to a person of any personal data pursuant to a request made under section 17 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.

38. (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 five hundred thousand shillings or to a term of imprisonment not exceeding five years, or to both.

(2) 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.

(3) 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.

Regulations.

39. (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.

Cap. 2.
No. 23 of 2013.

(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.

MEMORANDUM OF OBJECTS AND REASONS

Statement on the Objects and Reasons of the Bill

The principal object of the Bill is to protect personal data collected, used or stored by both private and public entities. The Bill recognizes that data protection forms part and parcel of the expectation of the right to privacy. This Bill **provides for the legal framework for protection of a person's privacy in instances where personal information is collected, stored, used or processed by another person. In Kenya the right to privacy is protected under Article 31 of the Constitution. Therefore, this Bill seeks to operationalise Article 31 of the Constitution, in particular Article 31(d) and (c).**

By providing for this right under the Constitution, is an indication as to the importance of the right to privacy. However, despite the importance attached to this right, the right is not absolute. It may be limited and must as of necessity be balanced against other competing rights and interests such as protecting the rights and freedoms of others, and maintaining law and order.

Part I of the Bill sets out definition of various terms used and application of the law. Part II outlines the objects and principles of protection of personal data. In particular, clause 4 sets out principles to guide the interpretation and application of the law, clause 6 sets out the circumstances the right to privacy regarding personal data can be limited. This Part also provide for the manner of collecting and processing personal data. Processing of special personal information, information relating to religious beliefs, race, health, trade union activities, data relating to a minor and political persuasions, is provided for under Part III of the Bill. It sets out the criteria for processing and who may process such information. Part IV on its part deals with oversight and implementation of the law. The Kenya National Commission on Human Rights will be the responsible institution for oversight and implementation, including investigating abuses. Final provisions encompassing offences and power for the Cabinet Secretary to make regulation are provided for under Part V of the Bill.

Due to massive development in the field of information, communication and technology experienced the world over and increase in collection of personal information by government and private bodies, the need to protect personal information has gained prominence. Therefore, there is urgent need to put in place rules to regulate the collection, use, storage and processing of personal information.

Statement on the delegation of legislative powers and limitation of fundamental rights and freedoms

Clause 36 of the Bill provides that the Cabinet Secretary may make Regulations for the better carrying out of the provisions of the Act. The Bill therefore delegates legislative powers to the county Cabinet Secretary.

The Bill proposes to limit the right to privacy under Article 31 of the Constitution respectively. Clause 6 of the Bill proposes to limit the right to privacy by providing that the right to privacy may be limited for the purpose of safeguarding fundamental rights and overriding legitimate interests. However, the limiting of this right must be in a manner that is least intrusive. The limitation of the right to privacy proposed in this Bill meets the requirements set out under Article 24(1) of the Constitution.

Statement on how the Bill concerns county governments

The Fourth Schedule to the Constitution provides for the functional areas of both the county governments and national government. In performance of this functions, and as of necessity, county governments as well as persons regulated by county governments collect, use and store personal information or data. This Bill seeks to put in place a legal framework for the protection of personal data that may be collected by private and public entities including county governments. The Bill therefore concerns county governments in terms of Articles 110(1)(a) of the Constitution in that it contains provisions that affect the functions and powers of the county governments as set out in the Fourth Schedule to the Constitution.

Statement that the Bill is not a money Bill within the meaning of Article 114 of the Constitution

The Bill is not a money Bill within the meaning of Article 114 of the Constitution.

Dated the 15th May, 2018.

GIDEON MOI,
Chairperson of the Committee on Information, Communication and Technology.