

THE DATA PROTECTION BILL, 2013

ARRANGEMENT OF CLAUSES

Clause

PART I - PRELIMINARY

- 1 — Short title.
- 2 — Interpretation.

PART II—OBJECTS AND PRINCIPLES ON PROTECTION OF PERSONAL INFORMATION ETC

- 3 — Objects of this Act.
- 4 — Principles of data protection.
- 5 — Right to protection of privacy.
- 6 — Limitation.
- 7 — Duty to notify.
- 8 — Collection of personal information.
- 9 — Exemption.
- 10 — Data processing.
- 11 — Protection and security of personal information.
- 12 — Access to information.
- 13 — Correction of information.
- 14 — Use of information.
- 15 — Storage of information.
- 16 — Misuse of information.

- 17 — Commercial use of data.
- 18 — Use of unique identifiers.
- 19 — Interference with personal information.

PART III—CONFERMENT ON THE COMMISSION OF OVERSIGHT AND ENFORCEMENT FUNCTIONS AND POWERS

- 20 — Role of the Commission.
- 21 — Functions of the Commission.

PART IV—COMPLAINTS, PROCEEDINGS AND SETTLEMENTS

- 22 — Inquiry into complaints.
- 23 — Proceedings on complaints.
- 24 — Settlement of complaints.

PART V—POWERS AND REMEDIES

- 25 — Powers and remedies of the Board on the complaint.
- 26 — Damages.

PART VI—MISCELLANEOUS PROVISIONS

- 27 — Protection against certain actions.
- 28 — Offences.

PART VII – PROVISIONS ON DELEGATED POWERS

- 29 — Regulations.

THE DATA PROTECTION BILL, 2013

A Bill for

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to regulate the collection, retrieval, processing, storage, use and disclosure of personal data 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, 2013.
- Interpretation. 2. In this Act, unless the context otherwise requires—
- “agency” includes public entities and private bodies;
- “Cabinet Secretary” means the Cabinet Secretary responsible for information and communications;
- No. 23 of 2011. “Commission” means the Commission on Administrative Justice established by section 3 of the Commission on Administrative Justice Act, 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;
- (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 equipment” means equipment used for processing data;

“data processor” means a person who processes personal information on behalf of a data controller but does not include an employee of a data controller who processes such information in the course of his or her employment;

“data subject” means a person who is the subject of personal data;

“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;

“electronic record” means a record generated in digital form by an information system, which may be transmitted within an information system or from one information system to another and stored in an information system or other medium;

“exempt information” has the meaning assigned to it under the law relating to access to information;

“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;
- (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 sent by the 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;

“private body” has the meaning assigned to it under the law relating to access to information;

“processing” means the performance of automatically logical or arithmetical operations on data and includes—

- (a) extracting any information constituting the data; and
- (b) in relation to a data processor, the use by a data controller of data equipment in the possession of the data processor and any other services provided by him for a data controller, but does not include an operation

performed solely for the purpose of preparing the text of documents;

“public entity” means—

- (a) any public office, as defined in Article 260 of the Constitution; or
- (b) any entity performing a function within a commission, office, agency or other body established under the Constitution;

“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; and

“secretary” has the meaning assigned to it by section 2 of the Commission on Administrative Justice Act, 2011.

PART II—OBJECTS AND PRINCIPLES OF PERSONAL INFORMATION PROTECTION ETC

Objects of this Act.

3. The objects of this Act are to—

- (a) give effect to the right of every person to privacy as provided under Article 31 (c) and (d) of the Constitution;
- (b) provide a framework for the protection of the right of a person to privacy of their personal data in relation to their private and family life; and
- (c) safeguard personal data from use or disclosure which is not in the interest of the data subject except in accordance with this Act.

Principles of data protection.

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

- (a) information shall be collected or stored if it is necessary for or directly related to a lawful, explicitly defined purpose and shall not intrude on the privacy of

The Data Protection Bill, 2013

the data subject to an unreasonable extent;

- (b) information shall be collected directly from and with the consent of the data subject;
- (c) the data subject shall be informed of the purpose of any collection of information and of the intended recipients of the information at the time of collection;
- (d) information shall not be kept for a longer period than is necessary for achieving the purpose for which it was collected;
- (e) 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;
- (f) reasonable steps shall be taken to ensure that the information processed is accurate, up-to-date and complete;
- (g) 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
- (h) 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 relating to their private and family life.

Limitation.

6. 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 but the right shall be limited in a manner that is least intrusive to the data subject.

Duty to notify.

7. (1) Before an agency collects personal information directly from a data subject, the agency shall take such steps as are in the circumstances reasonable to ensure that the data subject is aware of—

- (a) the fact that the information is being collected;
 - (b) the purpose for which the information is being collected;
 - (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 particular 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 or not the supply of the information 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 rights of access to, and correction of, personal information provided under section 12 and 13 of this Act.
- (2) An agency shall not collect personal information 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).

(4) An agency shall not be required to take the steps specified under subsection (1) 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.

(5) Where an agency collects information under subsection (4) to be used for a different purpose from the one for which the information was first collected, the agency shall notify the data subject of the use to which the information shall be put to.

(6) 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.

Collection of personal data.

8. (1) 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.

(2) An agency shall, in collecting personal data, ensure that—

(a) the information is collected only for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

(3) An agency which collects personal data may collect the information directly or indirectly from a data subject.

Exemptions.

9. An agency shall not be deemed to have collected personal data contrary to the provisions of section 8(2) if the agency proves, on reasonable grounds, that —

(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 for 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 or the Commission; or
 - (v) for purposes 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 be used in a manner which results in the identification of the data subject ;
 - (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; or
- (h) the information is collected pursuant to an authority granted under this Act or any other written law.

The Data Protection Bill, 2013

Data processing.

10. Where personal data concerning a data subject is to be subjected to automated or manual processing, the data subject shall have the right, upon request, to—

- (a) information relating to the person processing the data concerning him or her;
- (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; and
- (e) the rectification of incorrect data and the deletion of illegally processed data.

Protection and security of personal information.

11. An agency that holds personal data shall —

- (a) put in place such security safeguards that are reasonable in the circumstances to protect the data against —
 - (i) loss, damage and destruction; or
 - (ii) access, modification, negligent disclosure or use by an unauthorised person; and
- (b) where it is necessary for the data to be transmitted to a third party, in connection with the provision of a service to the agency, put in place measures to prevent the unauthorised use or disclosure of the data.

Access to data.

12. (1) Where an agency keeps personal data or where a person believes that an agency is keeping personal data relating to him or her, in a readily retrievable form, the data subject—

- (a) may obtain from the agency, a confirmation as to whether or not the agency holds such personal data; and
 - (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 law relating to access to information shall apply to subsection (1).

Correction of information.

13. (1) A data subject may, pursuant to Article 35 (2) of the Constitution, request an agency that holds personal data relating to him or her to correct or delete false or misleading data.

(2) An agency which holds personal data shall, if so requested by a data subject or on its own initiative, take steps to correct or delete false or misleading data.

(3) Where an agency rejects a request under subsection (1), it shall inform the data subject of the rejection and the reasons for the rejection in writing.

(4) An agency may reject a request under subsection (1) on the basis that the request does not amount to a request for the correction or deletion of data.

(5) Where an agency rejects a request by a data subject to correct data, the agency shall, if so requested by the data subject, attach to the data that it holds, in such manner as to be read together with that data, a statement provided by the data subject making the request.

(6) Where an agency attaches a statement provided by a data subject under subsection (5), that agency shall, if reasonably practicable, inform each person, body or agency to which the personal information has been disclosed of the attached statement.

(7) Where an agency receives a request pursuant to subsection (1), the agency shall inform the data subject of the action taken in relation to the request.

Use of information.

14. An agency that holds personal data shall take reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant and not misleading.

Storage of information.

15. An agency that holds personal data shall not keep the data for a longer period than is required for the purposes for which the information may lawfully be used.

The Data Protection Bill, 2013

Misuse of information.

16. 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.

17. 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.

Use of unique identifiers.

18. (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 information.

19. For the purposes of this Act, 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 one hundred thousand shillings or to imprisonment for a term not exceeding two years, or to both.

PART III – CONFERMENT ON THE COMMISSION OF OVERSIGHT AND ENFORCEMENT FUNCTIONS AND POWERS

Role of the Commission.

20. (1) The Commission shall oversee the implementation of and be responsible for the enforcement of this Act.

(2) In the performance of its functions under this Act, the Commission shall be guided by the national values and principles prescribed under the Constitution.

Functions of the Commission.

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

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

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

(c) take statements under oath in relation to any investigations it is undertaking.

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

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

(b) ensure that public entities have put in place adequate safeguards for the protection of personal data; and

(c) 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.

PART IV - COMPLAINTS, PROCEEDINGS AND SETTLEMENT

Inquiry into complaints.

22. (1) A data subject who is aggrieved by any 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.

(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) call for information or a report regarding such complaint from the relevant agency within such reasonable time as may be specified by the Commission; or
- (b) initiate such inquiry as it considers necessary, having regard to the nature of the complaint.

(6) Where an agency fails to submit the information or report within the time stipulated by the Commission under subsection (5)(a), the Commission may proceed to inquire into the complaint without the information or report.

(7) Where, upon receipt of the information or report from an 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.

23. The Commission may, upon receipt of a complaint under section 22, decline to take action or further action as the circumstances may require, if, in its opinion—

- (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) Despite subsection (1), the Commission may decline to take any further action on a complaint if, in the course of investigating the complaint, it appears to it, 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 the decline.

Settlement of complaints.

24. Where it appears to the Commission that based on a complaint or any written response made in relation to a complaint under section 23, that it may be possible to secure a settlement 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 and assurance.

PART V – POWERS AND REMEDIES

Powers and remedies of the Commission on the complaint.

25. (1) The Commission may, if in any proceedings under this Act, it is satisfied on a balance of probabilities that an action by the respondent amounts to an infringement of the right to the protection of data under this Act —

- (a) declare that the action of the respondent is a violation of the right to the protection of data in relation to the complainant;
- (b) make an order restraining the respondent from continuing or repeating the violation, from engaging in, or causing or permitting others to engage in conduct of a similar kind as that constituting the violation, or from engaging in

conduct of any similar kind specified in the order;

- (c) make an order for the performance by the respondent, of any act with a view to remedying the violation; or
- (d) make an order for such other relief as it considers appropriate.

(2) The Commission may, in any proceedings under this Act, and despite any other order that it may make –

- (a) award such costs against the respondent or the complainant as it may consider appropriate; or
- (b) decline to award any costs against any party.

(3) It shall not be a defence to any proceedings under this Act that the interference was unintentional or without negligence on the part of the respondent, but the Commission shall take the conduct of the defendant into account in determining the remedy to grant.

Damages.

26. The Commission may, in any proceedings under this Act, advise the complainant to seek damages in Court against the respondent for a violation of the right to the protection of data in respect of—

- (a) pecuniary loss suffered as a result of, and expenses reasonably incurred by the complainant in relation to the transaction or activity out of which the complaint arose;
- (b) a loss of any benefit, whether or not of a monetary kind, which the complainant might have reasonably been expected to obtain but for the infringement;
- (c) humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.

PART VI – MISCELLANEOUS PROVISIONS

Protection against certain actions.

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

- (a) no civil or criminal proceedings shall lie against the

agency in respect of availing the data, or for any consequences that may arise as a result of availing the data; and

- (b) no civil or criminal proceedings shall lie in respect of any publication of the availed data against the author of the information or any other person by reason of that author or other person having supplied the information to an agency.

(2) The availing or giving of access to a person of any personal data pursuant to a request made under section 12 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 availed or access is given.

Offences.

28. 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,

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.

PART VII – PROVISIONS ON DELEGATED POWERS

Regulations.

29. (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) for 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.

MEMORANDUM OF OBJECTS AND REASONS

The principle object of this Bill is to provide a framework for the protection of personal information that is collected by persons and processed automatically pursuant to Article 31 of the Constitution. The Bill recognizes that data protection in relation to personal information is a corollary to the expectation of privacy, a human right that is in keeping with best international practice. It also spells out the mechanisms for enhancing data protection. The Bill is borne of the realization that data protection is crucial for the promotion of e-transactions in the global digital economy where a lot of information is processed automatically.

While the Bill recognises the fact that every person has the right to privacy, as enshrined under Article 31 of the Constitution, with respect to their personal data, clause 6 limits this right for the purpose of safeguarding the overriding legitimate interests of the party concerned but also imposes an obligation to ensure that such limitation is exercised in a manner that is least intrusive to the data subject.

The Bill confers on the Cabinet Secretary the powers to make regulations under the Act for the purposes of operationalising the Act in order to implement the objectives set out in clause 3 of the Bill.

PART I of the Bill contains preliminary provisions which include the short title of the Bill and interpretation of terms used in the Bill.

PART II of the Bill contains provisions on principles of personal information protection. It sets out the objects of the Act and the principles on data protection that guide the application and interpretation of the Act. Clause 7 imposes on an agency, the duty to notify a data subject prior to collecting personal information from the data subject on facts including the collection of the information, the use to which the information shall be put and information relating to the agency collecting the information. It also outlines the manner in which information is to be collected, stored and used by an agency and the circumstances under which the collection of information would be exempt from such requirements. Clause 13 confers on a data subject the right to the correction or deletion of untrue information while clause 14 imposes an obligation on an agency to ensure that the personal data it holds is accurate and up to-date. This Part also imposes a duty on an agency that assigns a unique identifier to ensure that it is only assigned to persons whose identity is clearly established and not to disclose the identifier for purposes other than those for which the identifier was assigned.

The Bill contains the following Parts -

PART III outlines the role of the Commission on Administrative Justice in the implementation of the Act and also sets out its functions under this Act.

PART IV sets out the procedure for the lodging and determination of complaints, by the Commission, lodged by an aggrieved data subject under the Act. Clause 24 provides for the settlement of complaints by the Commission where it is of the opinion that the matter may be settled by the parties with or without conducting an inquiry under the Act.

PART V sets out the powers of the Commission and remedies that it may award in relation to proceedings instituted under the Act. Clause 26 provides for the award of damages by the Commission.

The Data Protection Bill, 2013

PART VI of the Bill contains miscellaneous provisions. Clause 27 provides for the protection of an agency that avails personal data in good faith and pursuant to the Act from criminal and civil liability while clause 28 provides for offences under the Act.

PART VII of the Bill confers on the Cabinet Secretary the powers to make regulations for the better carrying out of the provisions of the Act.

The enactment of this Bill will not occasion additional expenditure of public funds.

Dated the, 2013.

DR. FRED MATIANG'I,
Cabinet Secretary for
Information, Communications and Technology.

