LESOTHO
Government Gazette

Vol. 57 Wednesday – 22nd February, 2012 No. 19

CONTENTS

(See Supplement of the Gazette)

Published by the Authority of His Majesty the King
Price: M37.00

ACT NO. 5 OF 2012

Data Protection Act, 2011

Arrangement of Sections

Sections

ACT NO. 5 OF 2012

Data Protection Act, 2011

An Act to establish the Data Protection Commission, provide for principles for regulation of processing of personal information in order to protect and reconcile the fundamental and competing values of personal information privacy under this Act and sector-specific legislation and other related matters.

Enacted by the Parliament of Lesotho.

PART I – PRELIMINARY

Citation and commencement

1. This Act may be cited as the Data Protection Act, 2011 and shall come into operation on the date of publication in the Gazette.

Interpretation

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

"agent" in relation to personal data, means a person (other than an employee of the data controller) who processes the data on behalf of the data controller;

"automatic calling machine" means a machine that is able to do automated calls without human intervention;

"biometric" means a technique of personal identification that is based on physical characteristics including fingerprinting, DNA analysis, retinal scanning and voice recognition;

"child" means a natural person under the age of 18 years;

"code of conduct" means a code of conduct made and approved in terms of this Act;

"Commission" means the Data Protection Commission established

under section 6;

"Constitution" means the Constitution of Lesotho of 1993 as amended;

"data" means an unidentified data record, anonymised personal data or a fact about an unidentified individual;

"data controller" means a public or private body or any other person which or who, alone or together with others, determines the purpose of and means for processing personal information, regardless of whether or not such data is processed by that party or by an agent on its behalf;

"data subject" means an individual who is the subject of the personal data;

"de-identify" in relation to personal information of a data subject, means to delete any information that -

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; and

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject;

"electronic mail" or "e-mail" means any text, voice, sound or image message which is sent over a public communications network and can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"enforcement notice" means a notice issued under section 46;

"explicit consent" means any voluntary, specific and informed consent communicated expressly by spoken or written word in terms of which a data subject agrees to the processing of personal information relating to the data subject;

"filing system" means a set or collection of personal data records, structured either by reference to individuals or criteria relating to individuals,

in a way that specific information relating to a particular individual is readily accessible;

"implicit consent" means consent that is inferred from signs, actions, or facts, or by inaction or silence;

"information matching programme" means the comparison, whether manually or by means of any electronic or other device, of a document that contains personal information about ten or more data subjects with one or more documents which contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"member" means the member of Commission established under section 6;

"Minister" means the minister responsible for Home Affairs, Public Safety and of Parliamentary Affairs;

"opt-in-consent" means express consent, that is, where the data subject expressly agrees to something;

"opt-out-consent" means implied consent, that is, where the data subject is deemed to have consented to something;

"personal data or information" means data which relates to a living individual who can be identified -

(a) from that data; or

(b) from that data and other information which is in the possession, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"prescribed" means prescribed by the Regulations;

"private body" means a natural person or juristic person who or which carries or has carried on any trade, business or profession but only in that capacity;

"processing" means an operation or activity or any set of operations, whether or not by automatic means relating to -

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as blocking, degradation, erasure or destruction, of information;

"professional legal adviser" means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;

"public body" means -

(a) any department of state or administration in the national sphere of government or any council in the local sphere of government; or

(b) any other functionary or institution when -

(i) exercising a power or performing a duty in terms of the Constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

"public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

"public record" means a record that is accessible in the public domain

and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"record" means any recorded information -

(a) regardless of form or medium, including the following -

(i) writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing; or

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a data controller;

(c) whether or not it was created by the data controller; and

(d) regardless of when it came into existence;

"re-identify" in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that -

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable

method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

Application of the Act

3. This Act applies to a data controller -

(a) domiciled or having its principal place of business in Lesotho; or

(b) not domiciled or does not have its principal place of business in Lesotho and -

(i) uses automated or non-automated means in Lesotho; or

(ii) the automated or non-automated means are only used for forwarding personal information.

Exemptions

4. This Act does not apply to the processing of personal information-

(a) in the course of a purely personal or household activity;

(b) which has been de-identified to the extent that it cannot be reidentified; or

(c) by or on behalf of the State and involves national security and defence or public safety;

(d) solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression; or

(e) which has been exempted under this Act.

Sector specific legislation

5. (1) This Act does not affect the operation of any sector specific legislation which regulates the processing of personal information and is capable of operating concurrently with this Act.

(2) Where the sector specific legislation provides for the protection of personal information and such safeguards are more extensive than those set out under this Act, the extensive safeguards shall prevail.

PART II – DATA PROTECTION COMMISSION

Establishment of the Data Protection Commission

6. (1) There is established a Data Protection Commission which shall consist of a chairperson with legal expertise and five other members with expertise in social sector, business, information technology, finance and statistics.

(2) Members shall be appointed by the Prime Minister on the advice of the Minister.

(3) Before the members are appointed, the Minister shall invite interested parties through the media and by notice published in the Gazette to propose candidates within 30 days of the publication of such notice.

Disqualification from office

7. A person shall not be appointed as a member if the person -

(a) is a member of Parliament;

(b) is a councilor of a local authority;

(c) is an unrehabilitated insolvent; or

(d) has been convicted of -

(i) an offence under this Act;

(ii) a crime involving dishonesty; or

(iii) a crime and sentenced to a custodial sentence of more than 5 years.

Functions of the Commission

8. (1) The powers and duties of the Commission are to -

(a) promote by education and public awareness, an understanding and acceptance of information protection principles;

(b) make public statements in relation to any matter affecting protection of personal information of a data subject or of any class of data subjects;

(c) monitor and enforce compliance with the provisions of this Act by public and private bodies;

(d) undertake research into, and monitor developments in information processing and computer technology to ensure that any adverse effects of such developments on protection of personal information of data subjects are minimised and report to the Minister the results of such research and monitoring;

(e) examine any proposed policy or legislation which may affect the protection of personal information of data subjects, and report to the Minister the results of that examination;

(f) report, with or without request, to Parliament from time to time on any matter affecting protection of personal information of a data subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to personal information of a data subject;

(g) conduct an audit of personal information maintained by

a data controller for the purpose of ascertaining whether or not the information is maintained according to the information protection principles;

(h) monitor the use of unique identifiers of data subjects, and report to Parliament from time to time on the results of that monitoring;

(i) maintain, publish and provide copies of registers as required under this Act;

(j) receive and invite representations from members of the public on any matter provided for under this Act;

(k) consult and co-operate with other persons and bodies concerned with protection of personal information principles;

(l) advise the Minister or a public or private body on their obligations under this Act;

(m) receive, investigate and resolve complaints through mediation and reconciliation on alleged violations of the provisions of this Act, and report the findings and decisions to the complainants;

(n) report to Parliament from time to time on the desirability of the acceptance, by Lesotho, of any international instrument relating to the protection of personal information of a data subject;

(o) issue, approve, amend or revoke codes of conduct;

(p) make guidelines to assist public or private bodies to develop codes of conduct or to apply codes of conduct;

(q) review a decision made under an approved codes of conduct; and

(r) exercise and perform such other functions or powers as

conferred to it under this Act.

(2) The Commission may, from time to time, in the public interest or in the legitimate interests of any person or body of persons, publish reports relating generally to the exercise of the Commission's functions under this Act or to any case investigated by the Commission, whether or not the matters to be dealt with in any report have been the subject of a report to the Minister.

(3) For the purposes of this section, "time-to-time" means quarterly from the 1st of April each year.

Tenure of office

9. A member shall -

(a) hold office for 5 years from the date of appointment unless -

(i) the member resigns; or

(ii) the appointment is terminated by the Prime Minister after the member has been afforded an opportunity to make representations; or

(b) vacate office for inability to perform the functions of the Commission under this Act, whether arising from infirmity of body or mind or for misconduct.

Allowances of the members of the Commission

10. A member of the Commission shall be paid such allowances as the Minister may, in consultation with the Minister responsible for finance, determine.

Funds of the Commission

11. (1) The Funds of the Commission shall comprise of such amounts as shall be appropriated by Parliament from the Consolidated Fund.

(2) The Commission shall use the funds allocated under subsection (1) to carry out its functions as stipulated under this Act.

Audit of accounts

12. (1) The Commission shall submit, to the Minister, a budget for its annual operations not less than 6 months before the end of each financial year, which shall end on the 31st of March.

(2) The Commission shall, within 3 months after the end of each financial year, prepare a financial statement which reflects -

(a) the income and expenditure of the Commission during the preceding financial year; and

(b) a balance sheet showing the state of its assets, liabilities and financial position as at the end of that financial year.

(3) The Auditor-General shall audit the Commission's financial records each year.

(4) The Commission shall, within 6 months after the end of the financial year, submit the financial statement and audit report to the Minister for submission to Parliament.

Protection of Commission

13. The Commission or any person acting on behalf of or under the direction of the Commission shall not be civilly or criminally liable for anything done in good faith in the exercise or performance or purported exercise or performance of any power, duty or function of the Commission in terms of this Act.

Duty of confidentiality

14. A person acting on behalf of or under the direction of the Commission shall treat, as confidential, personal information which comes to his knowledge, except if the communication of such information is required by law or in the proper performance of his duties.

PART III – PROTECTION OF PERSONAL INFORMATION

Processing of personal information

15. (1) The processing of personal information shall be automated, processed and kept in -

(a) a filing cabinet; and

(b) electronic form.

(2) Personal information shall be processed if -

(a) the data subject provides explicit consent to the processing;

(b) processing is necessary for the conclusion or performance of a contract to which the data subject is a party;

(c) processing is necessary for compliance with a legal obligation to which the data controller is subject;

(d) processing is necessary to protect the legitimate interests of the data subject;

(e) processing is necessary for the proper performance of a public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied.

(2) A data subject may, on compelling legitimate grounds, raise a written objection to the processing of data relating to him on the grounds listed in subsection (1) with the Commission, and where the objection is upheld by the Commission, the data controller shall not process the data.

Minimality

16. Personal information may only be processed if, given the purpose for

which it is processed, it is adequate, relevant and not excessive.

Collection directly from the data subject

17. (1) A person shall collect personal information directly from the data subject, except where -

(a) the information is contained in a public record or has deliberately been made public by the data subject;

(b) the data subject has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(d) collection of the information from another source is necessary -

(i) to avoid prejudice to the maintenance or enforcement of the law and order;

(ii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

(iii) in the legitimate interests of national security; or

(iv) to maintain the legitimate interests of the data controller or of a third party to whom the information is supplied;

(e) compliance would prejudice a lawful purpose of the collection; or

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

Purpose specification and further processing limitation

18. (1) Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.

(2) The further processing of personal information shall be compatible with the purposes of collection if -

(a) the data subject has consented to the further processing of the information;

(b) the information is available in a public record or has deliberately been made public by the data subject;

(c) further processing is necessary -

(i) to avoid prejudice to the maintenance of the law or enforcement of the law and order;

(ii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(iii) in the legitimate interests of national security;

(d) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to-

(i) public health and safety; or

(ii) the life or health of the data subject or another individual; or

(e) the information is used for historical, statistical or research purposes and the data controller has established appropriate safeguards against the personal data being used for any other purposes.

Retention of records

19. (1) Subject to subsections (2) and (3), records of personal information shall not be retained any longer than a prescribed period, unless -

(a) retention of the record is required or authorised by law;

(b) the data controller reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties; or

(d) the data subject has consented to the retention of the record.

(2) Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes and the data controller has established appropriate safeguards against the personal data being used for any other purposes.

(3) A data controller which or who has used a record of personal information of a data subject to make a decision about the data subject shall -

(a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

(b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A data controller shall destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the data controller is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection (4) shall be done in a manner that prevents its recon-

struction in an intelligible form.

Security measures on integrity of personal information

20. (1) A data controller shall secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and authorised measures to prevent-

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the data controller shall take reasonable measures to -

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

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

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

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

(3) The data controller shall have due regard to generally accepted information security practices and procedures or professional rules and regulations which may apply generally or be required in the specific industry.

Information processed by an agent of the data controller

21. An agent or anyone processing personal information on behalf of a data controller shall -

(a) process such information only with the knowledge or authorisation of the data controller; and

(b) treat personal information which comes to their knowledge as confidential and shall not disclose it, unless required by law or in the course of the performance of their duties.

Security measures regarding information processed by an agent

22. (1) A data controller shall ensure that an agent which processes personal information for or on behalf of the data controller establishes and maintains the security measures referred to in this Act.

(2) The processing of personal information for a data controller by an agent on behalf of the data controller shall be governed by a written contract between the agent and the data controller, which requires the agent to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

(3) Where the agent is not domiciled or does not have its principal place of business in Lesotho, the data controller shall take reasonable steps to ensure that the agent complies with the laws relating to the protection of personal information of the territory in which the agent is domiciled.

Notification of security compromises

23. (1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an authorised person, the data controller, or any third party processing personal information under the authority of a data controller, shall notify -

(a) the Commission; and

(b) the data subject, unless the identity of such data subject cannot be established.

(2) The notification referred to in subsection (1) shall be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably

necessary to determine the scope of the compromise and to restore the integrity of the data controller's information system.

(3) The data controller shall delay notification to the data subject where the Lesotho Mounted Police Service, the National Security Service or the Commission determines that notification will impede a criminal investigation.

(4) The notification to a data subject referred to in subsection (1) shall be in writing and communicated to the data subject in one of the following ways -

(a) mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the party responsible for notification;

(d) published in the news media; or

(e) as may be directed by the Commission.

(5) A person making notification shall ensure that the notification provides sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including, if known to the data controller, the identity of the unauthorised person who may have accessed or acquired the personal information.

6) The Commission may direct a data controller to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, where the Commission has reasonable grounds to believe that the publicity would protect a data subject who may be affected by the compromise.

Quality of information

24. (1) The party responsible for collecting and processing of personal information shall take reasonably practicable steps to ensure that the personal

information is complete, accurate, not misleading and kept up to date where necessary.

(2) In taking the steps referred to in subsection (1), the party responsible for collecting and processing of personal information shall have regard to the purpose for which personal information is collected or further processed.

Notification to the Commission and to the data subject

25. (1) Where personal information is collected by the data controller directly from the data subject, the data controller shall take reasonable practicable steps to ensure that the data subject is aware of -

(a) the information being collected;

(b) the name and address of the data controller;

(c) the purpose for which the information is being collected;

(d) whether or not the supply of the information by the data subject is mandatory;

(e) the consequences of failure to provide the information;

(f) any law authorising or requiring the collection of the information; and

(g) any further information which is necessary having regard to the specific circumstances, such as the -

(i) recipient or category of recipients of the information;

(ii) nature or category of the information; and

(iii) existence of the right of access to and the right to rectify the information collected.

(2) The steps referred to in subsection (1) shall be taken -

(a) before the information is collected, unless the data subject is already aware of the information under subsection (1); or

(b) in any other case, as soon as reasonably practicable after it has been collected.

(3) A data controller which has previously taken the steps referred to in subsection (1) shall be in compliance with subsection (1) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information is unchanged.

(4) A data controller may not comply with subsection (1) where-

(a) the data subject has provided consent for the non-com--pliance;

(b) non-compliance would not prejudice the legitimate interests of the data subject as set out under this Act;

(c) non-compliance is necessary -

(i) to avoid prejudice to the maintenance or enforcement of the law and order;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue by the state;

(iv) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

(v) in the interests of national security;

(d) compliance would prejudice a lawful purpose of the collection;

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

(f) the information shall -

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for historical, statistical or research purposes.

(5) A data controller shall process personal information only upon notification to the Commission.

Access to and challenges of personal information

26. (1) A data subject who provides adequate proof of identity, shall have a right to request-

(a) a data controller to confirm, free of charge, whether or not the data controller holds personal information about the data subject; and

(b) from a data controller, personal information about the data subject held by the data controller, including information about the identity of all third parties, or categories of third parties who have or have had, access to the information -

(i) within a prescribed time;

(ii) at a prescribed fee;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) Where the data controller denies a data subject a request made in terms of subsection (1) above, the data subject shall be entitled to be given written reasons for the denial.

(3) A data subject shall have a right to challenge the written reasons for denial of requests made in terms of subsection (1).

(4) If, in accordance with subsection (1) (b), personal information is communicated to a data subject, the data subject shall be advised of the right in terms of section 27 to challenge the correctness of the information.

Correction of personal information

27. (1) A data subject shall free of charge have a right to challenge the correctness of information by requesting that a data controller -

(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroy or delete a record of personal information about the data subject that the data controller is no longer authorised to retain.

(2) A data controller shall, on receipt of a request in terms of subsection (1), take reasonable steps to investigate the challenge lodged and -

(a) correct, destroy or delete the information; or

(b) provide the data subject, with credible evidence in support of the correctness of the information.

(3) Where credible evidence has been provided under subsection (2) (b), the data subject may apply to the Commission to investigate the disputed information.

(4) Where the data controller has taken steps under subsection (2) (a) that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the data controller shall, within 7 working days, inform each person or body or data controller party to whom the personal information has been disclosed of those steps.

(5) The data controller shall notify a data subject, who has made a request in terms of subsection (1), of the outcome of the request within a period of 14 days of the making of the request.

Data controller to give effect to principles

28. The data controller shall ensure that the principles set out under this Act and all the measures that give effect to the principles are complied with.

Prohibition on processing of sensitive personal information

29. Unless specifically permitted under this Act, a data controller shall not process personal information concerning a -

(a) child who is subject to parental control in terms of the law; or

(b) data subject's spiritual, religious or philosophical beliefs, race or ethnic origin, trade union membership, political affiliation, health, sexual life or criminal behaviour.

PART IV – EXEMPTIONS FROM PROTECTION ON PROCESSING OF PERSONAL INFORMATION

Exemption on data subject's spiritual, religious or philosophical beliefs

30. (1) The prohibition on processing personal information of data subject's spiritual, religious or philosophical beliefs shall not apply if the processing is carried out by -

(a) spiritual or religious organisations, or independent sections of those organisations:

Provided that the information concerns data subjects belonging to those organisations;

(b) institutions founded on spiritual, religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or

(c) other institutions, if the processing is necessary to protect the spiritual, religious or philosophical welfare of the data subjects, unless they have indicated that they object to the processing.

(2) In cases under subsection (1) (a), the prohibition shall not apply to processing of personal information concerning the spirit, religion or philosophy of life of family members of the data subjects, where -

(a) the association concerned maintains regular contact with those family members in connection with its aims; and

(b) the family members have given explicit consent in writing to the processing.

(3) Personal information concerning a data subject's spiritual, religious or philosophical beliefs under subsections (1) and (2), shall not be supplied to third parties without the consent of the data subject.

Exemption on data subject's race

31. (1) The prohibition on processing personal information concerning a data subject's race shall not apply if the processing is carried out to -

(a) identify data subjects and only when this is essential for that purpose; and

(b) comply with the law.

(2) In the cases referred to under subsection (1), personal information shall not be supplied to third parties without the consent of the data subject.

Exemption on data subject's trade union membership

32. (1) The prohibition on processing personal information on a data subject's trade union membership, shall not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, where the processing is necessary to achieve the aims of the trade union or trade union federation.

(2) In the cases referred to under subsection (1), personal information shall not be supplied to third parties without the consent of the data subject.

Exemption on data subject's political affiliation

33. (1) The prohibition on processing personal information concerning a data subject's political affiliation, shall not apply to processing by an institution founded on political principles of the personal information of their members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution.

(2) In the cases under subsection (1), personal information shall not be supplied to third parties without the consent of the data subject.

Exemption on data subject's health or sexual life

34. (1) The prohibition on processing personal information on a data subject's health or sexual life, shall not apply to the processing by -

(a) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

(b) insurance companies, medical aid scheme administrators and managed healthcare organisations, where such processing is necessary for -

(i) assessing the risk to be insured by the insurance company or covered by the medical aid scheme and the data subject has not objected to the processing;

(ii) the performance of an insurance or medical aid agreement; or

(iii) the enforcement of any contractual rights and obligations;

(c) schools, where such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sexual life;

(d) institutions of probation, child protection or guardianship, where such processing is necessary for the performance of their legal duties;

(e) Commissioner of Correctional Service, where such processing is necessary in connection with the implementation of prison sentences or detention measures; or

(f) administrative bodies, pension funds, employers or institutions working for them, where such processing is necessary for -

(i) the implementation of the provisions of the law, pension regulations or collective agreements which create rights dependent on the health or sexual life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In cases under subsection (1), the information shall be processed by a data controller subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the data controller and the data subject.

(3) A data controller that is permitted to process information on a data subject's health or sexual life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, shall treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information.

(4) The prohibition on processing any of the categories of personal information shall not apply where it is necessary to supplement the processing of personal information on a data subject's health, with a view to the proper

treatment or care of the data subject.

(5) Personal information concerning inherited characteristics shall not be processed in respect of a data subject from whom the information concerned has been obtained, unless -

(a) a serious medical interest prevails; or

(b) the processing is necessary for the purpose of scientific research or statistics.

(6) The Commission may prescribe more detailed rules concerning the application of subsection (1)(b) and (f).

Exemption on data subject's criminal behaviour

35. (1) The prohibition on processing personal information on a data subject's criminal behaviour, shall not apply where the processing is carried out by a body charged by law with applying criminal law or by a data controller who have obtained that information in accordance with the law.

(2) The prohibition shall not apply to a data controller who processes the information for their own lawful purposes to -

(a) assess an application by a data subject in order to take a decision about, or provide a service to that data subject; or

(b) protect their legitimate interests in relation to criminal offences which have been or can reasonably be expected to be committed against them or against persons in their service.

(3) The processing of information concerning personnel in the service of the data controller shall take place in accordance with the rules established in compliance with the labour law.

(4) The prohibition on processing any of the categories of personnel information referred to in section 29 (b) shall not apply where such processing is necessary to supplement the processing of information on criminal behaviour

permitted under this section.

General exemption on sensitive personal information

36. Without prejudice to sections 29 to 35, the prohibition on processing personal information shall not apply where -

(a) processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

(d) the Commission has granted authority in terms of section 37 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy;

(e) processing is carried out with the consent of the data subject; or

(f) the information has deliberately been made public by the data subject.

Authorisation by the Commission

37. (1) The Commission may authorise a data controller to process personal information, where the Commission is satisfied that, in the circumstances of the case-

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or

(b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree,

any interference with the privacy of the data subject or third party that could result from such processing.

(2) The public interest referred to in subsection (1)(a) includes -

(a) the legitimate interests of State security;

(b) the prevention, detection and prosecution of offences;

(c) important economic and financial interests of the State or a public body;

(d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); or

(e) historical, statistical or research purposes and the data controller has established appropriate safeguards against the personal data being used for any other purposes.

(3) The Commission may impose reasonable conditions in respect of any authorisation issued under subsection (1).

Exemption for processing of personal data for historical, statistical and research purposes

38. (1) The further processing of personal information for historical, statistical and research purposes is exempt from all the information protection principles except -

(a) the principle regulating security safeguards; and

(b) the principle regulating information quality.

(2) The data controller shall establish appropriate safeguards against the use of the data for any other purpose.

No action by the Commission

41. (1) The Commission may, after receiving a complaint in terms of section 39, decide not to take action if, in the Commission's opinion -

(a) the length of time that has elapsed between the date on which the subject matter of the complaint arose and the date on which the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(b) the subject matter of the complaint is trivial;

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

(d) the complainant does not desire that action be taken or continued;

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

(f) the complaint relates to a matter governed by an approved code of conduct which makes provision for a complaints procedure, and the complainant has failed to use the complaints procedure as provided in that code; or

(g) the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body.

(2) Notwithstanding anything in subsection (1), the Commission may in its discretion decide not to take any further action on a complaint if, in the course of an investigation of the complaint, it appears to the Commission that, any further action is unnecessary or inappropriate.

(3) In any case where the Commission decides to take no action, or no further action, on a complaint, the Commission shall inform the complainant of that decision and the reasons for it.

Pre-investigations by the Commission

42. Before proceeding to investigate any matter in terms of this Part, the Commission shall inform the complainant and the data controller to whom the investigation relates of the -

(a) details of the subject matter of the investigation; and

(b) right of the data controller to submit to the Commission, within 14 days, a written response in relation to the subject-matter of the investigation.

Investigation proceedings of the Commission

43. (1) For the purpose of the investigation of a complaint, the Commission may -

(a) summon and enforce the appearance of persons before the Commission and compel them to give oral or written evidence on oath and to produce any records and things that the Commission considers necessary to enable it to investigate the complaint;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commission deems fit, whether or not it is or would be admissible in a court of law;

(d) apply to the Magistrate Court for a warrant to enter and search premises if there are reasonable grounds for suspecting that this Act has been contravened or an offence committed and evidence of that contravention or offence is to be found on the premises specified.

(2) A warrant issued under subsection (1)(d) shall be an authority for the Commission or any of its officers or staff, at any time within seven days of the date of issuing of the warrant to enter the premises as identified in the warrant and to search them, inspect, examine, operate and test any equipment

found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, material or equipment found there which may be used as evidence.

(3) A magistrate shall not issue a warrant under subsection (1)(d) unless the occupier has been notified by the Commission of the application for the warrant and has had an opportunity of being heard on the question whether the warrant should be issued.

Matters exempt from search and seizure

44. (1) Where the Commission has authorised the processing of personal information, the information is not subject to search and seizure.

(2) All privileged information is except from search and seizure.

Parties to be informed of developments during and result of investigation

45. If the Commission makes an investigation following a complaint, and -

(a) the Commission finds that no contravention of this Act has taken place;

(b) the Commission finds that a contravention has taken place;

(c) an enforcement notice is served in terms of section 46;

(d) a served enforcement notice is cancelled in terms of section 47;

(e) an appeal is lodged against the enforcement notice for cancellation or variation of the notice in terms of section 48; or

(f) an appeal against an enforcement notice is allowed, the notice is substituted or the appeal is dismissed, the Commission shall inform the complainant and the data controller in the manner prescribed of any development and the result of the investigation within a prescribed period.

Enforcement notice

46. (1) Where the Commission is satisfied that a data controller has contravened this Act, the Commission shall serve the data controller with an enforcement notice requiring the data controller to do either or both of the following -

(a) to take specified steps within a period specified in the notice, or to refrain from taking action; or

(b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

(2) An enforcement notice shall include -

(a) a statement indicating the nature of the contravention; and

(b) the right to appeal.

Cancellation of an enforcement notice

47. (1) A data controller on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Commission for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with this Act.

(2) If the Commission considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with this Act, it may cancel or vary the notice by written notice to the party on whom it was served.

Reviews and appeals

48. (1) A data controller on whom an enforcement notice has been served may, within 30 days of receiving the notice, apply to a court having com-

petent jurisdiction for the setting aside or variation of the notice.

(2) A complainant, who has been informed of the result of the investigation may, within 30 days of receiving the result, appeal to the Magistrate Court having jurisdiction against the result of the investigation.

Civil remedies

49. A data subject may institute a civil action for damages in a court having jurisdiction against a data controller for breach of any provision of this Act.

PART VI – GENERAL PROVISIONS

Unsolicited electronic communications

50. (1) In this section, "direct marketing" means communication by whatever means of any advertising or marketing material which is directed to particular data subjects.

(2) A data subject is entitled at any time by notice to a data controller to require the data controller to cease, or not to begin, processing of personal data in respect of which he is the data subject for the purposes of direct marketing.

(3) If the Commission is satisfied, on the application of any person who has given a notice under subsection (2), that the data controller has failed to comply with the notice, the Commission may order the data controller to take such steps for complying with the notice as the Commission thinks fit.

Automated decision making

51. (1) Subject to subsection (2), a person may not be subjected to a decision which has legal effect on him, or which affects him significantly, based solely on the automated processing of personal information intended to provide a profile of certain aspects of his personality or personal habits.

(2) The provisions of subsection (1) shall not apply where the decision -

(a) has been taken in connection with the conclusion or per-

formance of a contract, and -

(i) the request of the data subject in terms of the contract has been met; or

(ii) appropriate measures have been taken to protect the data subject's legitimate interests such as requiring a data controller to provide a data subject with sufficient information about the decision to enable him to make representations and allowing for a data subject to make representations about a decision referred to in subsection (1); or

(b) is governed by a law or code in which appropriate measures are specified for protecting the legitimate interests of data subjects.

Transfer of personal information outside Lesotho

52. A data controller in Lesotho shall not transfer personal information about a data subject to a third party who is in a foreign country unless -

(a) the recipient of the information is subject to a law, code of conduct or contract which -

(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles under this Act; and

(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the implementation of pre-contractual measures

taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; or

(e) the transfer is for the benefit of the data subject and -

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; or

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

Notifications

53. (1) A data controller shall notify the Commission of the processing of personal information to which this Act applies.

(2) The notification contemplated in subsection (1) shall contain the following particulars -

(a) the name and address of the data controller;

(b) the purpose of the processing;

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the personal information may be supplied;

(e) planned trans-border flow of personal information; and

(f) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the data controller to ensure the confidentiality, integrity and availability of the information which is to be processed.

(3) Subject to subsection (4), a data controller shall give notice each time personal information is received or processed.

(4) Changes in the name or address of the data controller shall be notified within one week, and changes to the notification which concern subsection (2)(b) to (f) shall be notified within one year of the previous notification, if they are of more than incidental importance.

(5) Any processing which departs from that which has been notified in accordance with the provisions of subsection (2)(b) to (f) shall be recorded and kept for at least three years.

(6) The Commission may -

(a) prescribe more detailed rules concerning the procedure for submitting notifications; and

(b) by notice exempt certain categories of information processing which are unlikely to infringe the legitimate interests of a data subject from the notification requirements referred to in this section.

(7) The Commission shall maintain an up-to-date register of the information processing notified to it.

Codes of conduct

54. (1) The Commission may, from time to time, issue, approve, amend or revoke a code of conduct.

(2) A code of conduct shall incorporate measures that give effect to all information protection principles, given the particular features of the sector or sectors of society in which the relevant data controller is operating.

(3) A code of conduct may apply in relation to any one or more of the following -

(a) specified information or class of information;

(b) specified body or class of bodies;

(c) specified activity or class of activities;

(d) specified industry, profession, or calling or class of industries, professions, or callings.

(4) A code of conduct may prescribe procedures for making and dealing with complaints alleging a breach of the code.

(5) The Commission shall keep a register of approved codes of conduct.

(6) The Commission may review the operation of an approved code of conduct.

Offences and penalties

55. A person who -

(a) hinders, obstructs or unlawfully influences the Commission or any person acting on behalf of or under the direction of the Commission in the performance of the Commission's duties and functions under this Act;

(b) breaches rules of confidentiality made under this Act;

(c) intentionally and unlawfully obstructs a person in the execution of a warrant issued under this Act;

(d) fails, without reasonable cause, to give a person executing a warrant or assistance as he may reasonably require for the execution of the warrant;

(e) violates any provisions of this Act or regulations made under this Act,

commits an offence and is liable, on conviction to a fine not exceeding M50 000.00 or to imprisonment for a period not exceeding 5 years or to both and if the offender is the juristic person the sentence shall be served by the Chief Executive Officer.

Regulations

56. The Minister may, on the recommendation of the Commission, make regulations generally for the purpose of giving effect to this Act.

Transitional arrangements

57. (1) Any person, who at the commencement date of this Act is processing any personal information shall, within two years of such date, bring such processing into conformity with this Act and notify the Commission in terms of section 53.

(2) The period of two years referred to in subsection (1) may be extended by the Minister by notice published in the Gazette to a maximum of three years.

NOTE

GOVERNMENT NOTICE NO. 10 OF 2012

Statement of Objects and Reasons of the Data Protection Act, 2011

(Circulated by the Authority of the Minister of Home Affairs, Public Safety and Parliamentary Affairs)

The object of the Bill is to provide for the establishment of a data protection regime in Lesotho. The fundamental position recognized by this Bill, on the other hand, is that privacy of personal information must be guaranteed. On the other hand free flow of information is a necessary feature of economic life. The Bill proposes provisions intended to balance protection of personal data rights against economic interests of the wider society.

The Bill makes provision for information protection principles that reflect international best practice on the rules that should apply to the processing of personal information. It also provides for exceptions to, exemptions and exclusions from compliance with the information protection principles, in so far as this is necessary to reconcile the right to personal information privacy with the right to receive and impart information. It further makes provision for regulation of automatic and manual processing of persona; and sensitive personal data by public and private bodies.

The Bill stipulates clearly defined rights of data subject and corresponding obligations of data controllers. Importantly, the Bill establishes the data protection commission, whose main function will be to oversee and ensure compliance with the Data Protection legislation. Additionally, the Bill makes provision for a legal infrastructure compatible with international best practices and rules especially compliance with the European Union's Data Protection Directive 95/46 EC since that will be a prerequisite for commercial; data flows between the European Union and the Kingdom of Lesotho. The compliance will further support trans-border flows of personal data proposes of trade, economic and social development.

Printed by the Government Printer, P.O. Box 268, Maseru 100 Lesotho