PERSONAL INFORMATION AND DATA PROTECTION BILL

ARRANGEMENT OF SECTIONS

Section:

PART - 1

PART 2

PART 3

PART 4

A BILL

FOR

AN ACT TO PROVIDE FOR REGULATIONS GOVERNING THE PROCESSING OF PERSONAL INFORMATION OF INDIVIDUALS, INCLUDING THE COLLECTION, HOLDING, USE OR DISCLOSURE OF SUCH INFORMATION BY PERSONS AND ORGANISATIONS OTHER THAN GOVERNMENT INSTITUTIONS IN A MANNER THAT RECOGNISES AND PROTECTS THE PERSONAL INFORMATION AND DATA OF INDIVIDUALS

BE IT ENACTED by the National Assembly of the Federal Republic of Nigeria as follows:

PART 1

Purpose

1. The purpose of this Act is to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organisations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Application

2. (1) This Act applies to every organisation in respect of personal information that

(*a*) the organisation collects, uses or discloses in the course of the organisation's commercial activities; or

(*b*) is about an employee of the organisation and that the organisation collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

(2) This Act does not apply to

(*a*) any government institution;

(*b*) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or

(*c*) any organisation in respect of personal information that the organisation collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.

Compliance with obligations

3. (1) Subject to sections 4, 5, 6 and 7, every organisation shall comply with the obligations set out in Schedule 1.

Meaning of "should"

(2) The word "should", when used in Schedule 1, indicates a recommendation and does not impose an obligation.

Appropriate purposes

(3) An organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Effect of designation of individual

4. The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organisation of the obligation to comply with the obligations set out in that Schedule.

Establishment of the Office of the Privacy Commissioner

4.1(1) There is hereby established for the purposes of this Act a Privacy Protection Office which shall be a public office.

(2) The head of the Privacy Protection Office shall be appointed by the President with the approval by resolution of the Senate, and the head of the office so appointed shall be known as the Privacy Commissioner.

(3) The Commissioner shall be a Legal Practitioner with at least 15 years standing at the Bar.

(4) Subject to the provision of this section, the Commissioner shall hold office for a term of four years, and may be re-appointed for another term of four years and no more.

(5) The Commissioner shall be assisted by such public officers as may be necessary.

(6) Every public officer referred to in subsection (5) shall be under the administrative control of the Commissioner.

(7) The Commissioner shall be responsible for the implementation and administration of this Act

Resignation or Removal of the Commissioner

(8) The Commissioner may-

(a) at any time resign from his office by notice in writing to the President; or

(b) be removed from office by the President with the approval by resolution of the Senate on the ground of-

i. inability to perform the functions of his office; or
ii. misconduct.

Commissioner to hold no other office

4.2 (1) The person appointed to be the Commissioner shall not, without the specific approval of the President

(a) hold any office of profit other than his office as Commissioner; or

(b) engage in any occupation for reward outside the functions of his office.

Filling of temporary vacancy

4.3 (1) Where the person appointed to be the Commissioner

(a) dies;

(b) resigns;

(c) is absent from Nigeria

(d) is removed from office;

(e) is for any other reason unable to perform the functions of his office,

then the President may, by notice in writing, appoint a person to act as the Commissioner until, as the case requires

(i) a new Commissioner is appointed under section 4.1 (3); or

(ii) the Commissioner resumes his office.

(2) A person appointed under subsection (1) to act as the Commissioner, whilst he is so appointed shall perform the functions and may exercise the powers of the Commissioner under this Act.

(3) Section 4.2(1) shall apply to a person appointed under subsection (1) to act as the Commissioner as if that person were the Commissioner.

Functions and Powers of the Commissioner

4.4 (1) The Commissioner shall-

(a) monitor and supervise compliance with the provisions of this Act;

(b) promote and assist bodies representing organisations to prepare codes of practice for guidance in complying with the provisions of this Act, in particular the data protection principles;

(c) promote awareness and understanding of, and compliance with, the provisions of this Act, in particular the data protection principles;

(d) examine any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal information and report the results of the examination to the person proposing the legislation;

(e) carry out inspections, including inspections of any personal information or data systems used by organisations;

(f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and computer technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal information;

(g) liaise and co-operate with any person in any place outside Nigeria -

i. performing in that place any functions which, in the opinion of the Commissioner, are similar (whether in whole or in part) to any of the Commissioner's functions under this Act; and
ii. in respect of matters of mutual interest concerning the privacy of individuals in relation to personal information; and

(h) perform such other functions as are imposed on the Commissioner under this Act or any other enactment.

(2) The Commissioner may do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and in particular but without prejudice to the generality of the foregoing, may-

(a) acquire and hold property of any description if in the opinion of the Commissioner such property is necessary for-

i. the accommodation of the Commissioner or of any prescribed officer; or
ii. the performance of any function which the Commissioner may perform, and, subject to the terms and conditions upon which such property is held, dispose of it;

(b) enter into, carry out, assign or accept the assignment of, vary or rescind, any contract, agreement or other obligation;

(c) undertake and execute any lawful trust which has as an object the furtherance of any function which the Commissioner is required or is permitted by this Act to perform or any other similar object;

(d) accept gifts and donations, whether subject to any trust or not;

(e) with the prior approval of the President, become a member of or affiliate to any international body concerned with (whether in whole or in part) the privacy of individuals in relation to personal data;

(f) exercise such other powers as are conferred on him under this Act or any other enactment.

(3) The Commissioner may make and execute any document in the performance of his functions or the exercise of his powers or in connection with any matter reasonably incidental to or consequential upon the performance of his functions or the exercise of his powers.

(4) The Commissioner may from time to time cause to be prepared and published by notice in the Gazette, for the guidance of organisations, guidelines not inconsistent with this Act, indicating the manner in which he proposes to perform any of his functions, or exercise any of his powers, under this Act.

Security Requirements

4.5 The Commissioner and every person acting on his behalf or under his direction who receives or obtains information relating to any investigation under this Act or any other enactment shall, with respect to access to and the use of that information, satisfy any security requirements applicable to, and take any oath of secrecy required to be taken by, persons who normally have access to and use of that information.

Collection without knowledge or consent

5. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organisation may collect personal information without the knowledge or consent of the individual only if

(*a*) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(*b*) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Nigeria;

(*c*) the collection is solely for journalistic, artistic or literary purposes;

(*d*) the information is publicly available; or

(*e*) the collection is made for the purpose of making a disclosure

(i) under subparagraph (3)(*d*)(i) or (*e*)(ii), or

(ii) that is required by or mandated by law.

Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organisation may, without the knowledge or consent of the individual, use personal information only if

(*a*) in the course of its activities, the organisation becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Nigeria or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(*b*) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(*c*) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organisation informs the Commissioner of the use before the information is used;

(*d*) it is publicly available; or

(*e*) it was collected under paragraph (1)(*a*), (*b*) or (*e*).

Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organisation may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(*a*) made to a barrister or solicitor who is representing the organisation;

(*b*) for the purpose of collecting a debt owed by the individual to the organisation;

(*c*) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(*d*) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Nigeria or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Nigeria or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Nigeria;

(e) made on the initiative of the organisation to an investigative body, a government institution or a part of a government institution; and the organisation

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Nigeria or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Nigeria or the conduct of international affairs;

(*f*) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organisation informs that individual in writing, without delay, of the disclosure;

(*g*) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organisation informs the Commissioner of the disclosure before the information is disclosed;

(*h*) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(*i*) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(*j*) of information that is publicly available;

(*k*) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Nigeria; or

(*l*) required or mandated by law.

Use without consent

(4) Despite clause 4.5 of Schedule 1, an organisation may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

Disclosure without consent

(5) Despite clause 4.5 of Schedule 1, an organisation may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(*a*) to (*k*).

Definitions under S.6

6 (1) The following definitions apply in this section.

"access" means to program, to execute programs on, to communicate with, to store data in, to retrieve data from, or to otherwise make use of any resources, including data or programs on a computer system or a computer network.

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer system" means a device that (or a group of interconnected or related devices one or more of which)

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"electronic address" means an address used in connection with

(*a*) an electronic mail account;

(*b*) an instant messaging account; or

(*c*) any similar account.

Collection of electronic addresses, etc.

(2) Paragraphs 5(1)(*a*), (*c*) and (*d*) and (2)(*a*) to (*d*) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of

(*a*) the collection of an individual's electronic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or

(*b*) the use of an individual's electronic address, if the address is collected by the use of a computer program described in paragraph (*a*).

Accessing a computer system to collect personal information, etc.

(3) Paragraphs 5(1)(*a*) to (*d*) and (2)(*a*) to (*d*) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of

(*a*) the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed in contravention of an Act of the National Assembly; or

(*b*) the use of personal information that is collected in a manner described in paragraph (*a*).

Written request

7. (1) A request under clause 4.9 of Schedule 1 must be made in writing.

Assistance

(2) An organisation shall assist any individual who informs the organisation that they need assistance in preparing a request to the organisation.

Time limit

(3) An organisation shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request.

Extension of time limit

(4) An organisation may extend the time limit

(*a*) for a maximum of thirty days if

(i) meeting the time limit would unreasonably interfere with the activities of the organisation, or

(ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or

(*b*) for the period that is necessary in order to be able to convert the personal information into an alternative format.

In either case, the organisation shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the Commissioner in respect of the extension.

Deemed refusal

(5) If the organisation fails to respond within the time limit, the organisation is deemed to have refused the request.

Costs for responding

(6) An organisation may respond to an individual's request at a cost to the individual only if

(*a*) the organisation has informed the individual of the approximate cost; and

(*b*) the individual has advised the organisation that the request is not being withdrawn.

Reasons

(7) An organisation that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this Act.

Retention of information

(8) Despite clause 4.5 of Schedule 1, an organisation that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Act that they may have.

When access prohibited

8 (1) Despite clause 4.9 of Schedule 1, an organisation shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party is severable from the record containing the information about the individual, the organisation shall sever the information about the third party before giving the individual access.

Limit

(2) Subsection (1) does not apply if the third party consents to the access or the individual needs the information because an individual's life, health or security is threatened.

Information related to paragraphs 5(3)(*c*), (*d*) or (e)

(2.1) An organisation shall comply with subsection (2.2) if an individual requests that the organisation

(*a*) inform the individual about

(i) any disclosure of information to a government institution or a part of a government institution under paragraph 5(3)(*c*), subparagraph 5(3)(*d*)(i) or (ii) paragraph 5(3)(*e*), or

(ii) the existence of any information that the organisation has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in paragraph 5(3)(*c*) or to a request made by a government institution or a part of a government institution under subparagraph 5(3)(*d*)(i) or (ii); or

(*b*) give the individual access to the information referred to in subparagraph (*a*)(ii).

Notification and response

(2.2) An organisation to which subsection (2.1) applies

(*a*) shall, in writing and without delay, notify the institution or part concerned of the request made by the individual; and

(*b*) shall not respond to the request before the earlier of

(i) the day on which it is notified under subsection (2.3), and

(ii) thirty days after the day on which the institution or part was notified.

Objection

(2.3) Within thirty days after the day on which it is notified under subsection (2.2), the institution shall notify the organisation whether or not the institution objects to the organisation complying with the request. The institution may object only if the institution is of the opinion that compliance with the request could reasonably be expected to be injurious to

(*a*) national security, the defence of Nigeria or the conduct of international affairs;

(*b*) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or

(c) the enforcement of any law of Nigeria or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

Prohibition

(2.4) Despite clause 4.9 of Schedule 1, if an organisation is notified under subsection (2.3) that the institution objects to the organisation complying with the request, the organisation

(*a*) shall refuse the request to the extent that it relates to paragraph (2.1)(*a*) or to information referred to in subparagraph (2.1)(*a*)(ii);

(*b*) shall notify the Commissioner, in writing and without delay, of the refusal; and

(*c*) shall not disclose to the individual

(i) any information that the organisation has relating to a disclosure to a government institution or a part of a government institution under paragraph 5(3)(*c*), subparagraph 5(3)(*e*)(i) or (ii) or paragraph 5(f) or to a request made by a government institution under either of those subparagraphs,

(ii) that the organisation notified an institution under paragraph (2.2)(*a*) or the Commissioner under paragraph (*b*), or

(iii) that the institution objects.

When access may be refused

(3) Despite the note that accompanies clause 4.9 of Schedule 1, an organisation is not required to give access to personal information only if

(*a*) the information is protected by solicitor-client privilege;

(*b*) to do so would reveal confidential commercial information;

(*c*) to do so could reasonably be expected to threaten the life or security of another individual;

(*d*) the information was collected under paragraph 5(1)(*b*);

(e) the information was generated in the course of a formal dispute resolution process; or

(*f*) the information was created for the purpose of making a disclosure under any law other than this Act or in the course of an investigation into a disclosure under that law.

However, in the circumstances described in paragraph (*b*) or (*c*), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the record containing any other information for which access is requested, the organisation shall give the individual access after severing.

Limit

(4) Subsection (3) does not apply if the individual needs the information because an individual's life, health or security is threatened.

Notice

(5) If an organisation decides not to give access to personal information in the circumstances set out in paragraph (3)(*d*), the organisation shall, in writing, so notify the Commissioner, and shall include in the notification any information that the Commissioner may specify.

Sensory disability

9. An organisation shall give access to personal information in an alternative format to an individual with a sensory disability who has a right of access to personal information under this Act and who requests that it be transmitted in the alternative format if

(*a*) a version of the information already exists in that format; or

(*b*) its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights under this Act.

PART 2

Remedies

Filing of Complaints

Contravention

10. (1) An individual may file with the Commissioner a written complaint against an organisation for contravening a provision of Part 1 or for not following a recommendation set out in Schedule 1.

Commissioner may initiate complaint

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commissioner may initiate a complaint in respect of the matter.

Time limit

(3) A complaint that results from the refusal to grant a request under section 7 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

Notice

(4) The Commissioner shall give notice of a complaint to the organisation against which the complaint was made.

Investigations of Complaints

Examination of complaint by Commissioner

11 (1) The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that

(*a*) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;

(*b*) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Nigeria, other than this Act; or

(*c*) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose.

Notification

(2) The Commissioner shall notify the complainant and the organisation that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons.

Compelling reasons

(3) The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate.

Powers of Commissioner

12 (1) In the conduct of an investigation of a complaint, the Commissioner may

(*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;

(*b*) administer oaths;

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

(*d*) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organisation on satisfying any security requirements of the organisation relating to the premises;

(*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the investigation.

Dispute resolution mechanisms

(2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

Delegation

(3) The Commissioner may delegate any of the powers set out in subsection (1) or (2).

Return of records

(4) The Commissioner or the delegate shall return to a person or an organisation any record or thing that they produced under this section within 10 days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

Certificate of delegation

(5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(*d*).

Discontinuance of Investigation

Reasons

13 (1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that

(*a*) there is insufficient evidence to pursue the investigation;

(*b*) the complaint is trivial, frivolous or vexatious or is made in bad faith;

(*c*) the organisation has provided a fair and reasonable response to the complaint;

(*d*) the matter is already the object of an ongoing investigation under this Act;

(*e*) the matter has already been the subject of a report by the Commissioner;

(*f*) any of the circumstances mentioned in paragraph 11(1)(*a*), (*b*) or (*c*) apply; or

(*g*) the matter is being or has already been addressed under a procedure referred to in paragraph 11(1)(*a*) or (*b*).

Notification

(2) The Commissioner shall notify the complainant and the organisation that the investigation has been discontinued and give reasons.

Commissioner's Report

Contents

14 (1) The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains

(*a*) the Commissioner's findings and recommendations;

(*b*) any settlement that was reached by the parties;

(*c*) if appropriate, a request that the organisation give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and

(*d*) the recourse, if any, that is available under section 12.

Report to parties

(2) The report shall be sent to the complainant and the organisation without delay.

Hearing by Court

Application

15. (1) A complainant may, after receiving the Commissioner's report or being notified under subsection 13(2) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Part 1, in subsection 3(3) or 7(6) or (7) or in section 8.

Time of application

(2) A complainant must make an application within 45 days after the report or notification is sent or within any further time that the Court may, either before or after the expiry of those 45 days, allow.

For greater certainty

(3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 10(2) as to complaints referred to in subsection 10(1).

Commissioner may apply or appear

16. The Commissioner may, in respect of a complaint that the Commissioner did not initiate,

(*a*) apply to the Court, within the time limited by section 15, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;

(*b*) appear before the Court on behalf of any complainant who has applied for a hearing under section 15; or

(*c*) with leave of the Court, appear as a party to any hearing applied for under section 15.

Remedies

17. The Court may, in addition to any other remedies it may give,

(*a*) order an organisation to correct its practices in order to comply with sections 3 to 9;

(*b*) order an organisation to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (*a*); and

(*c*) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Summary hearings

18. (1) An application made under section 15 or 16 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so.

Precautions

(2) In any proceedings arising from an application made under section 15 or 16, the Court shall take every reasonable precaution, including, when appropriate, receiving representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organisation would be authorised to refuse to disclose if it were requested under clause 4.9 of Schedule 1.

PART 3

Audits

To ensure compliance

19 (1) The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organisation if the Commissioner has reasonable grounds to believe that the organisation is contravening a provision of Part 1 or is not following a recommendation set out in Schedule 1, and for that purpose may

(*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit, in the same manner and to the same extent as a superior court of record;

(*b*) administer oaths;

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

(*d*) at any reasonable time, enter any premises, other than a dwelling-house, occupied by the organisation on satisfying any security requirements of the organisation relating to the premises;

(*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the audit.

Delegation

(2) The Commissioner may delegate any of the powers set out in subsection (1).

Return of records

(3) The Commissioner or the delegate shall return to a person or an organisation any record or thing they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

Certificate of delegation

(4) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(*d*).

Report of findings and recommendations

20 (1) After an audit, the Commissioner shall provide the audited organisation with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.

Reports may be included in annual reports

(2) The report may be included in a report made under section 27.

PART 4

General

Confidentiality

21 (1) Subject to subsections (2) to (6), 11(2), 13(2), 14(2), 20(1), 24(3) and 25(1) and section 27, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Act.

Public interest

(2) The Commissioner may make public any information relating to the personal information management practices of an organisation if the Commissioner considers that it is in the public interest to do so.

Disclosure of necessary information

(3) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to

(*a*) conduct an investigation or audit under this Act; or

(*b*) establish the grounds for findings and recommendations contained in any report under this Act.

Disclosure in the course of proceedings

(4) The Commissioner may disclose, or may authorise any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of

(*a*) a prosecution for an offence under section 31;

(*b*) a prosecution for perjury in respect of a statement made under this Act;

(*c*) a hearing before the Court under this Act; or

(*d*) an appeal from a decision of the Court.

Disclosure of offence authorised

(5) The Commissioner may disclose to the Attorney General of Nigeria, information relating to the commission of an offence against any law of Nigeria on the part of an officer or employee of an organisation if, in the Commissioner's opinion, there is evidence of an offence.

Commissioner not Competent Witness

22 The Commissioner or person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part in any proceeding other than

(*a*) a prosecution for an offence under section 31

(*b*) a prosecution for perjury in respect of a statement made under this Act;

(*c*) a hearing before the Court under this Act; or

(*d*) an appeal from a decision of the Court.

Protection of Commissioner

23 (1) No criminal or civil proceedings shall lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith as a result of the performance or exercise or purported performance or exercise of any duty or power of the Commissioner under this Act.

Libel or slander

(2) For the purposes of any law relating to libel or slander,

(*a*) anything said, any information supplied or any record or thing produced in good faith in the course of an investigation or audit carried out by or on behalf of the Commissioner under this Act is privileged; and

(*b*) any report made in good faith by the Commissioner under this Act and any fair and accurate account of the report made in good faith for the purpose of news reporting is privileged.

Consultations with States

24. (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under the legislation of a State, has functions and duties similar to those of the Commissioner with respect to the protection of such information.

Agreements or arrangements with States

(2) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) in order to

(*a*) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;

(*b*) undertake and publish research or develop and publish guidelines or other instruments related to the protection of personal information;

(*c*) develop model contracts or other instruments for the protection of personal information that is collected, used or disclosed nationally or internationally; and

(*d*) develop procedures for sharing information referred to in subsection (3).

Sharing of information with States

(3) The Commissioner may, in accordance with any procedure established under paragraph (2)(*d*), share information with any person referred to in subsection (1), if the information

(*a*) could be relevant to an ongoing or potential investigation of a complaint or audit under this Act or legislation of a State that has objectives that are similar to this Act; or

(*b*) could assist the Commissioner or that person in the exercise of their functions and duties with respect to the protection of personal information.

Purpose and confidentiality

(4) The procedures referred to in paragraph (2)(*d*) shall

(*a*) restrict the use of the information to the purpose for which it was originally shared; and

(*b*) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

Disclosure of information to foreign state

25 (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(*b*), disclose information referred to in subsection (2) that has come to the Commissioner's knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Act to any person or body who, under the legislation of a foreign state, has

(*a*) functions and duties similar to those of the Commissioner with respect to the protection of personal information; or

(*b*) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.

Information that can be shared

(2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes

(*a*) would be relevant to an on-going or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of this Act; or

(*b*) is necessary to disclose in order to obtain from the person or body information that may be useful to an on-going or potential investigation or audit under this Act.

Written arrangements

(3) The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that

(*a*) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(*a*) or (*b*);

(*b*) restricts the use of the information to the purpose for which it was originally shared; and

(*c*) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

Arrangements

(4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to

(*a*) provide for cooperation with respect to the enforcement of laws protecting personal information, including the sharing of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested;

(*b*) establish procedures for sharing information referred to in subsection (2);

(*c*) develop recommendations, resolutions, rules, standards or other instruments with respect to the protection of personal information;

(*d*) undertake and publish research related to the protection of personal information;

(*e*) share knowledge and expertise by different means, including through staff exchanges; or

(*f*) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.

Promoting the purposes of this Act

26. The Commissioner shall

(*a*) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Act;

(*b*) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the minister in charge of commerce and industry;

(*c*) encourage organisations to develop detailed policies and practices, including organisational codes of practice, to comply with sections 3 to 8; and

(*d*) promote, by any means that the Commissioner considers appropriate, the purposes of this Act.

Annual and Special Reports

27 (1) The Commissioner shall, within three months after the end of each calendar year, submit to the National Assembly a report concerning the activities of his office and the application of this Act.

(2) The Commissioner may, at any time, make a special report to the National Assembly referring to and commenting on any matter within the scope of the powers, duties and functions of the Commissioner, if, in his opinion, the matter is of such urgency or importance that a report thereon should not be deferred until the time provided for transmission of the annual report of the Commissioner under subsection (1).

(3) Every report to the National Assembly made by the Commissioner under subsections (1) and (2) shall be made by being transmitted to the President of the Senate and to the Speaker of the House of Representatives for tabling in those Houses.

Consultation

(2) Before preparing the report, the Commissioner shall consult with those persons in the States who, in the Commissioner's opinion, are in a position to assist the Commissioner in reporting respecting personal information that is collected, used or disclosed nationally or internationally.

Regulations

28 (1) The President may make regulations

(*a*) specifying, by name or by class, what is a government institution or part of a government institution for the purposes of any provision of this Act;

(b) specifying, by name or by class, what is an investigative body for the purposes of paragraph 5(3)(e) or (k);

(c) specifying information or classes of information for the purpose of paragraph 5(1)(*d*), (2)(*d*) or (3)(*j*); and

(d) for carrying out the purposes and provisions of this Act.

Orders

(2) The President may, by order, if satisfied that legislation of a State that is substantially similar to this Act applies to an organisation, a class of organisations, an activity or a class of activities, exempt the organisation, activity or class from the application of this Act in respect of the collection, use or disclosure of personal information that occurs within that State.

Whistleblowing

29 (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision of Part 1, may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

Confidentiality

(2) The Commissioner shall keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

Prohibition

30 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise put to a disadvantage an employee, or deny an employee a benefit of employment, by reason that

(*a*) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of this Act;

(*b*) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of this Act;

(*c*) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of this Act not be contravened; or

(*d*) the employer believes that the employee will do anything referred to in paragraph (*a*), (*b*) or (*c*).

Saving

(2) Nothing in this section impairs any right of an employee either at law or under an employment contract or collective agreement.

Definition

(3) In this section, “employee” includes an independent contractor and “employer” has a corresponding meaning.

Offence and punishment

31. Every person who knowingly contravenes subsection 7(8) or 30(1) or who obstructs the Commissioner or the Commissioner’s delegate in the investigation of a complaint or in conducting an audit is guilty of an offence punishable on summary conviction and liable to a fine not exceeding N1,000,000 (One Million, Five Hundred Thousand Naira Only).

Review of Act by National Assembly

32(1) The administration of this Act shall, every five years after this Act comes into force, be reviewed by the committee of the House of Representatives, or of both Houses of the National Assembly, that may be designated or established by the National Assembly for that purpose.

Review and Report

(2) The committee shall undertake a review of the provisions and operation of this Act and shall, within a year after the review is undertaken or within any further period that the House of Representatives may authorize, submit a report to the House of Representatives that includes a statement of any changes to this Act or its administration that the committee recommends.

Definitions

33 (1) The definitions in this subsection apply in this Act.

“alternative format”, with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information.

“commercial activity” means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

“Commissioner” means the Privacy Commissioner appointed under Section 4.1(3).

“Court” means the Federal High Court.

“federal work, undertaking or business” means any work, undertaking or business that is within the legislative authority of the National Assembly. It includes

(*a*) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Nigeria;

(*b*) a railway, canal, telegraph or other work or undertaking that connects a State with another State, or that extends beyond the limits of a State;

(*c*) a line of ships that connects a State with another State, or that extends beyond the limits of a State;

(*d*) a ferry between a State and another State or between a State and a country other than Nigeria;

(*e*) aerodromes, aircraft or a line of air transportation;

(*f*) a radio broadcasting station;

(*g*) a bank;

(h) an insurance company

(*i*) a work that, although wholly situated within a State, is before or after its execution declared by the National Assembly to be for the general advantage of Nigeria or for the advantage of two or more States;

(j) a work, undertaking or business within the exclusive legislative authority of the National Assembly;

"Minister" means the Minister of justice.

"Nigeria" means the Federal Republic of Nigeria.

"organisation" includes an association, a partnership, a company, a person and a trade union.

"personal health information", with respect to an individual, whether living or deceased, means

(*a*) information concerning the physical or mental health of the individual;

(*b*) information concerning any health service provided to the individual;

(*c*) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(*d*) information that is collected in the course of providing health services to the individual; or

(*e*) information that is collected incidentally to the provision of health services to the individual.

"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation.

"record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

"State" means a State of the Federal Republic of Nigeria.

Notes in Schedule 1

(2) In this Act, a reference to clause 4.3 or 4.9 of Schedule 1 does not include a reference to the note that accompanies that clause.

34. This Act may be cited as the Personal Information and Data Protection Act

SCHEDULE 1

PRIVACY PRINCIPLES FOR THE PROTECTION OF PERSONAL INFORMATION

4.1 Principle 1 — Accountability

An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation's compliance with the following principles.

4.1.1

Accountability for the organisation's compliance with the principles rests with the designated individual(s), even though other individuals within the organisation may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organisation may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organisation to oversee the organisation's compliance with the principles shall be made known upon request.

4.1.3

An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organisations shall implement policies and practices to give effect to the principles, including

(*a*) implementing procedures to protect personal information;

(*b*) establishing procedures to receive and respond to complaints and inquiries;

(*c*) training staff and communicating to staff information about the organisation's policies and practices; and

(*d*) developing information to explain the organisation's policies and procedures.

4.2 Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.

4.2.1

The organisation shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organisations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organisation to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organisations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organisation. In such cases, the organisation providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organisation will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organisation wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organisations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organisation shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organisation may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organisations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that

the organisation, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organisation can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organisation seeks consent may vary, depending on the circumstances and the type of information collected. An organisation should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organisations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(*c*) consent may be given orally when information is collected over the telephone; or

(*d*) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organisation shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.

4.4.1

Organisations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organisations shall specify the type of information collected as part of

their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organisations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1

Organisations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organisations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organisation may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organisations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

An organisation shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organisations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;

(*b*) organisational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(*c*) technological measures, for example, the use of passwords and encryption.

4.7.4

Organisations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 — Openness

An organisation shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organisations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organisation's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(*a*) the name or title, and the address, of the person who is accountable for the organisation's policies and practices and to whom complaints or inquiries can be forwarded;

(*b*) the means of gaining access to personal information held by the organisation;

(*c*) a description of the type of personal information held by the organisation, including a general account of its use;

(*d*) a copy of any brochures or other information that explain the organisation's policies, standards, or codes; and

(*e*) what personal information is made available to related organisations (e.g., subsidiaries).

4.8.3

An organisation may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organisation may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organisation may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organisation shall inform an individual whether or not the organisation holds personal information about the individual. Organisations are encouraged to indicate the source of this information. The organisation shall allow the individual access to this information. However, the organisation may choose to make sensitive medical information available through a medical practitioner. In addition, the organisation shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organisation to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organisation should attempt to be as specific as possible. When it is not possible to provide a list of the organisations to which it has actually disclosed information about an individual, the organisation shall provide a list of organisations to which it may have disclosed information about the individual.

4.9.4

An organisation shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organisation uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organisation shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion,

or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organisation. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 — Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation's compliance.

4.10.1

The individual accountable for an organisation's compliance is discussed in Clause 4.1.1.

4.10.2

Organisations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organisations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

An organisation shall investigate all complaints. If a complaint is found to be justified, the organisation shall take appropriate measures, including, if necessary, amending its policies and practices.