

Model Data Protection Code	Implementation and Operational Guidelines
<p>1. Scope This Model Code describes the minimum requirements for the protection of personal information in the form of electronic data ("personal data"). Any applicable law must be considered in implementing these requirements.</p> <p>1.1 The objective of this Model Code is to assist organisations in developing and implementing policies and procedures to be used when managing personal data.</p>	<p>The Model Code is intended to provide a broad and flexible framework based on the principles of the OECD Guidelines. The principles have been framed in general terms so that they may be applied across sectors by a wide range of organisations.</p> <p>However, it is also recognised that the types of organisations and their use of data may vary significantly between sectors. If this is the case, the Model Code may, as an alternative, be used as a template upon which businesses or industries may base more industry-specific data protection rules.</p>
<p>1.2 Where appropriate, the following data processing activities may be exempted:</p> <ul style="list-style-type: none"> (a) Processing required by any law or by the order of a court; (b) Processing by any person purely for that person's family, household or personal affairs (including recreational purposes); (c) Processing purely for journalistic, artistic or literary purposes; (d) Processing by any organisation directly relating to a current or former employment relationship between the organisation and the individual; (e) Any processing operations which are necessary to safeguard: <ul style="list-style-type: none"> (i) National and public security; (ii) National defence; (iii) The prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (iv) An important national economic or financial interest, including monetary, budgetary and taxation matters; (v) A monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority; 	<p>Despite the Code's exemption of employment data, organisations may opt to restrict this exemption only to such processing activities necessary for the purposes of carrying out their obligations under the employment relationship.</p> <p>As the business environment evolves, the Code will be reviewed periodically to ensure that it is aligned to leading practices and the interests and needs of consumers and businesses.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>(vi) The protection of the individual or of the fundamental liberties of others under the Constitution; and</p> <p>(f) Processing for research or statistical purposes, provided the results of the research or any resulting statistics are not made available in a form which identifies any individual.</p>	
<p>1.3 The Model Code applies to the processing of personal data whether or not by electronic means.</p>	<p>“Personal data” is defined below as data in electronic form (see definition below at Clause 2).</p> <p>Data kept in non-electronic form subsequently converted into electronic form will be subject to the Model Code from that point onwards.</p> <p>Electronic data when presented in non-electronic form (e.g. by being printed) is still subject to the Model Code.</p> <p>Organisations are of course free to additionally subject their data kept in non-electronic form to the operation of the code, on a voluntary basis.</p>
<p>1.4 The Model Code applies to any personal data which are processed or controlled by the organisation, regardless of whether the data are transferred out of Singapore.</p> <p>The Model Code applies in favour of all persons, whether resident in Singapore or not, whose data are or have been processed by the organisation.</p>	<p>Data may be transferred by an organisation out of Singapore. If control is retained within the organisation (e.g. transfer to a data bureau solely for processing and return to the organisation for use), the data remain subject to the Model Code.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>2. Definitions</p> <p>The following definitions apply in this Model Code:</p> <p>Collection — the act of gathering, acquiring, or obtaining personal data from any source, and whether directly or indirectly by any means.</p>	
<p>Consent — voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organisation seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.</p>	
<p>Control — in relation to an organisation, refers to its power to determine the purposes for which data are processed, and the manner in which they are processed.</p>	
<p>Disclosure — making personal data available to others outside the organisation.</p>	
<p>Individual – refers to the individual to whom the personal data relates.</p>	
<p>Organisation — a term used in the Model Code that includes associations, businesses, charitable organisations, clubs, institutions, professional practices, and unions.</p>	

Model Data Protection Code	Implementation and Operational Guidelines
<p>Personal data — data, whether true or not, in an electronic form, which relate to a living person who can be identified —</p> <ul style="list-style-type: none"> (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the organisation. 	<p>Persons are identifiable not only by their names but also by their pictures, their telephone numbers, or by some special identification number (e.g. NRIC and Passport numbers), etc.</p> <p>"Personal data" may include an individual's:</p> <ul style="list-style-type: none"> • name, age, weight, height • NRIC/FIN number • medical records • income, purchases and spending habits • race, ethnic origin and colour • blood type, DNA code, fingerprints • marital status and religion • education • home address and phone number <p>"Data" refers to data which are in a form which can be potentially understood by the recipient (e.g. encrypted data without the key would not be "data" because they cannot be understood). But they would become "data" if they are capable of being decrypted.</p>
<p>Processing — any operation or set of operations performed upon personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.</p>	
<p>Third Party — any party other than the individual, the organisation or any person who processes personal data on behalf of the individual or the organisation.</p>	
<p>Use — refers to the treatment and handling of personal data within an</p>	

Model Data Protection Code	Implementation and Operational Guidelines
organisation.	
<p>3. General Requirements</p> <p>3.1</p> <p>The 10 principles in Part 4 are interrelated. Organisations adopting this Model Code shall adhere to all 10 principles as a whole.</p>	<p>Clauses which use prescriptive language (i.e. the words "shall" or "must") are requirements. The use of the word "should" indicates a recommendation.</p>
<p>3.2</p> <p>Each principle is elaborated upon in the sub-paragraphs that follow it. These sub-paragraphs are intended to help readers understand the significance and the implications of the principles.</p>	
<p>3.3</p> <p>Provided the minimum requirements are met, organisations may adapt this Model Code to meet their specific circumstances by:</p> <ul style="list-style-type: none"> (a) defining how they subscribe to the 10 principles; (b) developing an organisation-specific code; and (c) modifying the text to provide organisation-specific examples. <p>For example, policies and procedures may vary, depending upon whether the personal data relate to members, employees, customers, or other persons.</p>	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4. Principles</p> <p>4.1 Principle 1 — Accountability</p> <p><i>An organisation is responsible for personal data in its possession or custody.</i></p> <p><i>Where the personal data is under the control of the organisation, the organisation shall, in addition, designate a person or persons who are accountable for the organisation’s compliance with the following principles.</i></p> <p>4.1.1</p> <p>Where data are to be transferred to someone (other than the individual or the organisation or its employees), the organisation shall take reasonable steps to ensure that the data which is to be transferred will not be processed inconsistently with this Model Code.</p>	<p>A member of the senior management team should be made responsible for the management and co-ordination of the information resources, policies and procedures of the organisation. The person must have authority, the support of senior management and have an in-depth knowledge of information management techniques, computer and telecommunications.</p> <p>This responsibility could be assigned to the Chief Privacy Officer (‘CPO’) or Chief Information Officer (‘CIO’) of the organisation or its equivalent.</p> <p>The restrictions on the onward transfers of personal data under this principle apply to transfers to another organisation whether the organisation is located in Singapore or not. These restrictions ensure that personal data continue to enjoy similar levels of protection even when exported. This clause incorporates the restrictions under Principle 11 (Transborder Data Flows) of the earlier draft Model Data Protection Code developed by the National Internet Advisory Committee (NIAC). Principle 11 is based on the restrictions on international transfers of personal data set out in Article 25 of the EU Directive (95/46/EC).</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.1.2 Accountability for the organisation's compliance with the principles rests with the designated person(s), even though other persons within the organisation may be responsible for the day-to-day collection and processing of personal data. In addition, other persons within the organisation may be delegated to act on behalf of the designated person(s).</p>	<p>Generally, some responsibilities of the designated person (in addition to any duties imposed by law) are:</p> <ul style="list-style-type: none"> • To establish and keep up-to-date policies and procedures to protect personal data; • To prepare impact assessments of both current and proposed information systems on data protection; • To ensure the implementation of the organisation's data protection policies and procedures by other organisations to which data processing functions are out-sourced. • To educate employees of the organisation on the importance of data protection; and • To stay abreast of technical and legal developments in this field in order to enable management to maintain the highest reasonable security standards.
<p>4.1.3 The identity of the person(s) designated by the organisation to oversee the organisation's compliance with the principles shall be made known upon request.</p>	
<p>4.1.4 Organisations shall implement policies and procedures to give effect to the principles. These may include:</p> <ol style="list-style-type: none"> (a) implementing policies and procedures to protect personal data; (b) establishing policies and procedures to receive and respond to complaints and inquiries; (c) training staff and communicating to staff data about the organisation's policies and procedures; and (d) providing relevant information to explain the organisation's policies and procedures. 	<p>Like infocomm security, data protection procedures and practices can be woven into the work processes of the organisation as good practices.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.2 Principle 2 —Specifying Purposes</p> <p><i>The purposes for which personal data are collected shall be specified by the organisation.</i></p>	<p>Identifying purposes for the collection of personal data forces organisations to focus their data collection on only data which is necessary for the stated purposes. This is critical to the Limiting Collection principle (Principle 4), which requires an organisation to collect only that data necessary for the purposes that have been identified.</p> <p>This principle should not be viewed as a constraint on the organisation. Since data collection and maintenance may be costly, identifying purposes is the first step in reducing operating costs.</p> <p>The difficulty of developing new uses of data beyond those identified in the very beginning can be overcome by an organisation having a clear vision and far-sighted business plans.</p> <p>This principle is also closely linked to the Limiting Use, Disclosure, and Retention principle (Principle 5).</p>
<p>4.2.1</p> <p>These purposes shall be documented.</p>	<p>The organisation shall document the purposes for which personal data are collected in order to comply with the Openness principle (Principle 8) and the Individual Access and Correction principle (Principle 9).</p>
<p>4.2.2</p> <p>The identified purposes should be specified to the person from whom the personal data is collected or to the individual (“the relevant party”). Depending upon the way in which the data are collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.</p>	<p>Statements of purpose should not be so broad as to make this principle nugatory (e.g. “to serve you better” or “for your benefit”).</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.2.3</p> <p>The organisation shall specify these purposes at or before the time the data are collected or, in the event that this is not practicable, as soon thereafter as is reasonable.</p>	
<p>4.2.4</p> <p>When personal data that have been collected are to be used for a purpose not previously specified, the new purpose shall be specified to the relevant party prior to use. The use of such data is still subject to the other principles in this Code.</p>	<p>See Clause 4.2.2 for the “relevant party”.</p> <p>“Specified to the relevant party” does not necessarily mean that personal notice must be given. Depending on the circumstances (e.g. the sensitivity of the data, its intended use, etc), such purpose can be specified through any reasonable and convenient means, e.g. printed notices on applications, poster displays at entrances to premises, on-line for internet transactions, or even a general publication.</p>
<p>4.2.5</p> <p>The purposes must be specified in such a manner that the individual can reasonably understand why the data is being collected and how the data will be used or disclosed.</p>	<p>Organisations shall use reasonable efforts to ensure that individuals are made aware of these purposes. Brochures explaining these purposes should be comprehensible. Persons collecting personal data should also be able to explain the purposes for which the data are being collected.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.3 Principle 3 — Consent</p> <p><i>The knowledge and consent of the individual are required for the collection, use, or disclosure of personal data to a third party, save where the following exceptions apply:</i></p> <p><i>Collection without knowledge or consent of the individual is permitted where:</i></p> <p>(a) <i>All of the following apply:</i></p> <ul style="list-style-type: none"> <i>i) the collection is clearly in the interest of the individual;</i> <i>ii) it is impracticable to obtain the consent of the individual to that collection; and</i> <i>iii) if it were practicable to obtain such consent, the individual would be likely to give it.</i> <p>(b) <i>Collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the data where such collection pertains to an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;</i></p> <p>(c) <i>Data is being collected in an emergency that threatens the life, health or security of a person; or</i></p> <p>(d) <i>Collection is of data which is generally available to the public.</i></p> <p><i>Use without knowledge or consent of the individual is permitted where:</i></p> <p>(e) <i>All of the following apply:</i></p> <ul style="list-style-type: none"> <i>i) the use is clearly in the interest of the individual;</i> <i>ii) it is impracticable to obtain the consent of the individual to that use; and</i> <i>iii) if it were practicable to obtain such consent, the individual would be likely to give it.</i> <p>(f) <i>Data is used in the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;</i></p>	<p>Informed or enlightened consent is the underpinning of fair information practices. Sometimes, the purpose for which data are collected is obvious and aligns so closely with the individual's expectations that consent can be implied. Nonetheless, the individual has a right to know what the principal purposes of the collection are, and whether there are any other intended purposes for the data.</p> <p>In certain circumstances personal data can be collected, used, or disclosed without the knowledge and consent of the individual. These exceptions are set out in the Code, e.g. when data are 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 data. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.</p> <p>On the use of cookies, if users are properly informed (i.e. what information is being collected, by whom and for what) and give their consent whether expressed or implied to their use, this is not a breach of the Code, provided of course that the organisation also ensures that the cookies do not collect information indiscriminately, as this may breach the Limiting Collection principle (Principle 4).</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>(g) <i>Data is being used in an emergency that threatens the life, health or security of a person; or</i></p> <p>(h) <i>Use of data which is generally available to the public.</i></p> <p><i>Disclosure to a third party without knowledge or consent of the individual is permitted where:</i></p> <p>(i) <i>All of the following apply:</i></p> <ul style="list-style-type: none"> <i>i) the disclosure is clearly in the interest of the individual;</i> <i>ii) it is impracticable to obtain the consent of the individual to that disclosure; and</i> <i>iii) if it were practicable to obtain such consent, the individual would be likely to give it.</i> <p>(j) <i>Disclosure is made to a solicitor representing the organisation;</i></p> <p>(k) <i>Disclosure is necessary for the purposes of establishing, exercising or defending legal rights;</i></p> <p>(l) <i>Disclosure is to a government agency that has made a lawful request for the data;</i></p> <p>(m) <i>Disclosure is made to a person who needs the data because of an emergency that threatens the life, health or security of a person;</i></p> <p>(n) <i>Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;</i></p> <p>(o) <i>Disclosure is of data which is generally available to the public in that form; or</i></p> <p>(p) <i>Disclosure is reasonable for purposes related to the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being or is about to be committed.</i></p>	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.3.1</p> <p>Consent shall be obtained by the organisation at or before the time of processing except that where an organisation wants to use data for a purpose not previously identified, consent with respect to use or collection may be obtained after the data are collected but before use.</p>	<p>See also Clause 4.2.4 on use of data for new purposes.</p>
<p>4.3.2</p> <p>An organisation may not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of data beyond that required to fulfil the specified, and legitimate purposes.</p>	<p>The organisation may want to weigh the implications of using opt-out procedures very carefully, as the public may be averse to such procedures, which might be seen as analogous to reverse-marketing tactics (where the onus is on the individual to opt out of new services for which he might be charged). Nonetheless, opt-out procedures might still be acceptable, and even desirable, from the consumer's point of view, depending on the sensitivity of and intended uses for the personal data (e.g. own use vs. third party use, etc).</p>
<p>4.3.3</p> <p>The form of the consent sought by the organisation may vary, depending upon the circumstances and the type of data. In determining the form of consent to use, organisations shall take into account the sensitivity of the data.</p>	<p>Although some data (for example, medical records and income records) are almost always considered to be sensitive, any datum can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive data. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.</p>
<p>4.3.4</p> <p>Consent does not have to be obtained by the organisation directly from the individual. Consent can be given by an authorised representative (such as a legal guardian or a person having power of attorney).</p>	<p>Organisations that do not have a direct relationship with the individual may not always be able to seek consent directly from the individual. 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 whether expressed or</p>

Model Data Protection Code	Implementation and Operational Guidelines
	implied before disclosing personal data.
<p>4.3.5 Consent shall not be obtained through deception or by providing misleading or incomplete information.</p>	<p>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 data given to a health-care professional would be given to a company selling health-care products, unless consent were obtained.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.3.6</p> <p>The way in which an organisation seeks consent may vary, depending on the circumstances and the type of data collected. An organisation should generally seek express consent when the data are likely to be considered sensitive. Implied consent would generally be appropriate when the data are less sensitive.</p>	<p>Individuals can give consent in many ways. For example:</p> <ul style="list-style-type: none"> (a) an application form may be used to seek consent, collect data, and inform the individual of the use that will be made of the data. 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 data to third parties; (c) consent may be given orally when data are collected over the telephone; or (d) any other opt-out measures which are fair and reasonable.
<p>4.3.7</p> <p>An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The individual may only be subjected to consequences because of this decision where the information is required to fulfil the specified, and legitimate purposes set out by the organisation (e.g. in the absence of the data on which to assess an individual's creditworthiness, an organisation may refuse to extend credit to him). The organisation should inform the individual of the implications of such withdrawal.</p>	<p>Individuals should have the opportunity to opt out of data collection and to request deletion of that personal data that have already been collected.</p>
<p>4.4 Principle 4 — Limiting Collection</p> <p><i>Except as provided below, the collection of personal data shall be limited to that which is necessary for the purposes specified by the organisation.</i></p> <p><i>Data shall be collected by fair and lawful means.</i></p>	<p>From a perspective of business efficacy, it is advantageous to collect only data which are necessary for a serious business purpose, as this translates into reduced costs for data collection and maintenance.</p> <p>Organisations should specify the type of data collected as part of their data-handling policies and practices, in accordance with the</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p><i>Collection beyond purposes specified is permitted where:</i></p> <p>(a) <i>All of the following apply:</i></p> <ul style="list-style-type: none"> <i>i) the collection is clearly in the interest of the individual;</i> <i>ii) it is impracticable to obtain the consent of the individual to that collection; and</i> <i>iii) if it were practicable to obtain such consent, the individual would be likely to give it.</i> <p>(b) <i>Collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the data where such collection pertains to an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;</i></p> <p>(c) <i>Data is being collected in an emergency that threatens the life, health or security of a person;</i></p> <p>(d) <i>Collection is of data which is generally available to the public; or</i></p> <p>(e) <i>The individual consents to the collection.</i></p> <p>4.4.1</p> <p>Organisations shall not collect personal data indiscriminately. Both the amount and the type of data collected shall be limited to that which is necessary to fulfil the purposes identified.</p>	<p>Openness principle (Principle 8).</p> <p>The requirement that personal data be collected by fair and lawful means is intended to prevent organisations from collecting data by misleading or deceiving individuals about the purpose for which data are being collected. This requirement implies that consent with respect to collection must not be obtained through deception.</p> <p>The situations in which data may be collected beyond purposes specified are generally similar to the situations in which data may be collected without the knowledge or consent of the individual under the Consent principle (Principle 3).</p> <p>This principle is linked closely to the Specifying Purposes principle (Principle 2) and the Consent principle (Principle 3).</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.5 Principle 5 — Limiting Use, Disclosure, and Retention</p> <p><i>Except as provided below, personal data shall not be used or disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure.</i></p> <p><i>Subject to any applicable legal requirements, personal data shall be retained only as long as necessary for the fulfilment of those purposes.</i></p> <p><i>Use beyond the purposes for which it was collected is permitted where:</i></p> <p>(a) <i>All of the following apply:</i></p> <ul style="list-style-type: none"> <i>i) the use is clearly in the interest of the individual;</i> <i>ii) it is impracticable to obtain the consent of the individual to that use; and</i> <i>iii) if it were practicable to obtain such consent, the individual would be likely to give it.</i> <p>(b) <i>Data is used in the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;</i></p> <p>(c) <i>Data is being used in an emergency that threatens the life, health or security of a person;</i></p> <p>(d) <i>Use of data which is generally available to the public; or</i></p> <p>(e) <i>The individual consents to the use.</i></p> <p><i>Disclosure beyond the purposes of collection is permitted where:</i></p> <p>(f) <i>All of the following apply</i></p> <ul style="list-style-type: none"> <i>i) the disclosure is clearly in the interest of the individual;</i> <i>ii) it is impracticable to obtain the consent of the individual to that use; and</i> 	<p>The situations in which data may be used or disclosed beyond purposes specified are generally similar to the situations in which data may be used or disclosed without knowledge or consent of the individual under the Consent principle (Principle 3).</p> <p>The principle also deals with issues of records retention and destruction. Organisations should develop policies regarding the retention of records. This retention period must be long enough to allow individuals an opportunity to exercise their right of access under Individual Access and Correction principle (Principle 9).</p> <p>Once this retention period expires, the information should be destroyed, made anonymous or deleted in a manner which prevents its re-creation. It should be noted that a normal file deletion does not meet the requirement of the Safeguards principle (Principle 7) since several utilities are available to restore it.</p> <p>These guidelines should include minimum and maximum retention periods. An organisation may be subject to legal requirements with respect to retention periods.</p> <p>Personal data that are no longer required to fulfil the specified purposes or any legal requirements should be destroyed, erased, or made anonymous.</p> <p>This principle is closely linked to the Consent principle (Principle 3), the Identifying Purposes principle (Principle 2), and the Individual Access and Correction principle (Principle 9).</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p><i>iii) if it were practicable to obtain such consent, the individual would be likely to give it.</i></p> <p><i>(g) Disclosure is made to a solicitor representing the organisation;</i></p> <p><i>(h) Disclosure is necessary for the purposes of establishing, exercising or defending legal rights;</i></p> <p><i>(i) Disclosure is to a government agency that has made a lawful request for the data;</i></p> <p><i>(j) Disclosure is made, on the initiative of the organisation, to an investigative body appointed by the organisation, or to a government agency for investigative purposes;</i></p> <p><i>(k) Disclosure is made to a person who needs the data because of an emergency that threatens the life, health or security of a person;</i></p> <p><i>(l) Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;</i></p> <p><i>(m) Disclosure is of data which is generally available to the public in that form; or</i></p> <p><i>(n) Disclosure is made by an investigative body and the disclosure is reasonable for purposes related to the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being or is about to be committed.</i></p> <p>4.5.1</p> <p>Organisations using personal data for a new purpose shall document this purpose in accordance with the Specifying Purposes principle (Principle 2).</p>	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.5.2</p> <p>Organisations should develop guidelines and implement procedures with respect to the retention and destruction of personal data. Personal data that have been used to make a decision about an individual shall be retained long enough to allow the individual access to the data after the decision has been made.</p>	
<p>4.6 Principle 6 — Accuracy</p> <p><i>Personal data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.</i></p> <p>4.6.1</p> <p>Personal data should be collected directly from the individual as far as it is practicable to do so.</p>	<p>This principle reflects the relationship between data accuracy and the intended use of the information and seeks to minimise the possibility that inappropriate data may be used to make a decision about the individual.</p> <p>The extent to which personal data shall be accurate, complete, and up-to-date will depend upon the use of the data, taking into account the interests of the individual.</p> <p>Personal data that are used on an ongoing basis, including data that are disclosed to third parties, should generally be accurate and up-to-date, unless limits to the degree of accuracy are clearly set out.</p> <p>Collection of personal data directly from individual normally improves the quality of the information collected.</p>
<p>4.6.2</p> <p>An organisation shall request updates of personal data from individuals only where the update is necessary to fulfil the purposes for which the data were collected.</p>	<p>The purpose of this principle is to prevent data collectors from routinely collecting updates of personal data needlessly, or on the pretext of regular updates.</p>

Model Data Protection Code	Implementation and Operational Guidelines
4.6.3 The organisation, in complying with this principle, may take into consideration the extent to which compliance is reasonable.	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.7 Principle 7 — Safeguards</p> <p><i>Personal data shall be protected by appropriate security safeguards.</i></p> <p>4.7.1</p> <p>The security safeguards shall protect personal data against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification. Organisations shall protect personal data regardless of the format in which they are held.</p>	
<p>4.7.2</p> <p>The nature and extent of the safeguards will vary depending on: -</p> <ul style="list-style-type: none"> (a) the sensitivity of the data that have been collected; (b) the amount, distribution, and format of the data; (c) the method of storage; (d) the state of technological development; and (e) the cost and reasonableness of implementation of the safeguards. 	<p>Security measures should be commensurate with the risks and consequences of disclosure.</p> <p>More sensitive data should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in the Consent principle (Principle 3).</p>
<p>4.7.3</p> <p>The methods of protection may include one or more of the following:</p> <ul style="list-style-type: none"> (a) physical measures, for example, secured filing cabinets and restricted access to offices; (b) organisational measures, for example, security clearances and limiting access on a "need-to-know" basis; (c) technological measures, for example, the use of passwords and encryption, as may be available, appropriate and reasonable from time to time. 	<p>Access to personal data within an organisation must be allowed only on a need-to-know basis. Generally speaking, this should be based on a two-part test:</p> <ul style="list-style-type: none"> • The employee must need access to the information in the performance of their duties; and • The access by the employee must be in support of a legitimate business function of the organisation.
<p>4.7.4</p> <p>Organisations shall make their employees aware of the importance of</p>	

Model Data Protection Code	Implementation and Operational Guidelines
maintaining the confidentiality of personal data.	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.7.5</p> <p>Reasonable care shall be used in the disposal or destruction of personal data, to prevent unauthorised parties from gaining access to the data.</p>	<p>This is closely linked to the Limiting Use, Disclosure and Retention principle (Principle 5).</p>
<p>4.8 Principle 8 — Openness</p> <p><i>An organisation shall make readily available information about its policies and procedures for handling personal data.</i></p> <p>4.8.1</p> <p>Organisations shall be open about their policies and procedures with respect to the management of personal data. Individuals should be able to acquire information about an organisation's policies and procedures without unreasonable effort. Such information shall be made available in a form that is generally understandable.</p>	<p>An organisation may make information on its policies and procedures 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.</p> <p>Internet web pages are very effective for disseminating such information. Where an organisation's data protection policy is displayed on its web site, translation (e.g. into the 4 official languages) is not necessary so long as the policy is set out in the same language medium as the web site itself.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.8.2</p> <p>The information made available shall include —</p> <ul style="list-style-type: none"> (a) the name/title and address of the person who is accountable for the organisation's policies and procedures and to whom complaints or inquiries can be forwarded; (b) the means of gaining access to personal data held by the organisation; (c) a description of the type of personal data held by the organisation, including a general account of their use; (d) a description of the organisation's policies or standards; and (e) what personal data are generally made available or are likely to be made available to other organisations, including related organisations such as subsidiaries. 	
<p>4.9 Principle 9 — Individual Access and Correction</p> <p><i>Subject to the following exceptions, an individual shall upon his request be informed of the existence, use, and disclosure of his personal data and shall be given access to that data. An individual shall be able to challenge the accuracy and completeness of his personal data and have them amended as appropriate. The reasons for denying access should be provided to the individual upon request.</i></p> <p><i>The organisation shall refuse the request where:</i></p> <ul style="list-style-type: none"> (a) <i>Providing access would be likely to reveal personal data about another person, unless</i> <ul style="list-style-type: none"> - <i>the said person consents to the access; or</i> - <i>the individual needs the information because a person's life, health or security is threatened,</i> <i>provided that where the data about the said person is severable from the record containing the data about the individual, the organisation shall sever the data about the said person and shall</i> 	<p>In certain situations, an organisation may not be able to provide access to all the personal data it holds about an individual. These exceptions are set out in this Model Code.</p> <p>Notwithstanding that contractual reasons may form the basis of a “legal” reason to refuse access under (d), an organisation may not unfairly deprive an individual of access, e.g. by entering into agreements which oblige the organisation not to reveal such data, even to the individual.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p><i>provide the individual access; or</i></p> <p><i>(b) An investigative body or government agency, upon notice being given to it of the individual's request, objects to the organisation's complying with the request in respect of its disclosures made to or by that investigative body or government agency;</i></p> <p><i>The organisation may refuse the request where:</i></p> <p><i>(c) Data is protected by solicitor-client privilege;</i></p> <p><i>(d) It would reveal data that cannot be disclosed for public policy, legal, security, or commercial proprietary reasons, Provided that where the personal data about the individual is severable from the record that cannot be disclosed for public policy, legal, security or commercial proprietary reasons, the organisation shall sever the data and give the individual access;</i></p> <p><i>(e) It would threaten the life, health or security of a person;</i></p> <p><i>(f) Data was collected under 4.3(b) (generally, collection pertaining to an investigation of a breach of an agreement or the law);</i></p> <p><i>(g) Complying with the request would be prohibitively costly to the organisation; or</i></p> <p><i>(h) The request is frivolous or vexatious.</i></p>	<p>Frivolous and vexatious requests include those that are:</p> <ul style="list-style-type: none"> • trivial and made for amusement's sake; • made as a means of pursuing some unrelated grievance against the organisation; • repeated requests for access to the same personal data. <p>However, an organisation should not consider a request for access as frivolous or vexatious simply because it is irritating.</p>

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.9.1</p> <p>Upon request, an organisation shall inform a person whether or not the organisation holds personal data about the person. Organisations are encouraged to indicate the source of this data. The organisation shall allow the individual access to this data. In addition, the organisation should provide confirmation as to whether or not data relating to him are being processed and data at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.</p>	<p>Notwithstanding the general rule, an organisation may choose to make sensitive medical data available through a medical practitioner.</p>
<p>4.9.2</p> <p>An organisation shall verify the identity of the individual concerned before granting access. Further, the individual may be required to provide sufficient data to permit an organisation to provide an account of the existence, use and disclosure of personal data. The data provided shall only be used for this purpose.</p>	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.9.3</p> <p>In providing an account of recipients or categories of recipients to which it has disclosed personal data 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 data about an individual, the organisation should provide a list of organisations to which it may have disclosed data about the individual.</p>	
<p>4.9.4</p> <p>An organisation shall respond to an individual's request within a reasonable time and may charge a reasonable fee for providing the information or data requested for. The requested data shall be provided or made available in a form that is generally understandable. For example, if the organisation uses abbreviations or codes to record data, an explanation shall be provided.</p>	<p>Organisations may develop their own policy as to who should bear the costs for access and what reasonable fees may be charged, and under what circumstances.</p>
<p>4.9.5</p> <p>When an individual successfully demonstrates the inaccuracy or incompleteness of personal data, the organisation shall amend the data as required within a reasonable time. Depending upon the nature of the data challenged, amendment may involve the correction, deletion, or addition of data. Where appropriate, the amended data shall be transmitted to recipients having access to the data in question.</p>	<p>Organisations may develop their own policy as to who should bear the costs of correction. The best practice however is that such costs should not be passed on to consumers.</p>
<p>4.9.6</p> <p>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</p>	

Model Data Protection Code	Implementation and Operational Guidelines
challenge shall be transmitted to recipients currently having access to the data in question.	

Model Data Protection Code	Implementation and Operational Guidelines
<p>4.10 Principle 10 — Challenging Compliance</p> <p><i>An individual shall be able to address a challenge concerning compliance with the above principles to the designated person or persons accountable for the organisation's compliance.</i></p> <p>4.10.1</p> <p>Organisations shall put mechanisms and processes in place to receive and address complaints or inquiries about their policies and procedures relating to the handling of personal data. The complaint process should be simple and accessible.</p>	<p>The person accountable for an organisation's compliance is discussed in Accountability principle (Principle 1).</p> <p>Mechanisms to receive complaints may include providing a telephone number or enabling the organisation's web site to receive complaints or inquiries. Mechanisms to address complaints may include internal or external complaint review processes.</p>
<p>4.10.2</p> <p>Organisations shall inform persons who make inquiries or lodge complaints of the existence of relevant complaint mechanisms.</p>	
<p>4.10.3</p> <p>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 procedures.</p>	

Model Data Protection Code	Implementation and Operational Guidelines
<p>5. Transitional Provisions</p> <p>Upon adoption of this Model Code, the Code applies to all personal data already in existence. However, organisations may be allowed a transitional period of up to one year to comply with Individual Access and Correction principle (Principle 9).</p>	<p>This transitional provision allows flexibility to organisations to adopt this Model Code in phases, at a pace sustainable according to their particular needs. While a transitional period of up to one year is allowed, organisations which are operationally ready to comply with the Individual Access and Correction principle (Principle 9) are encouraged to do so as soon as possible.</p> <p>If these transitional provisions (with or without modifications as to the transitional period) are adopted by the organisation, a notice to this effect should be clearly set out in its data protection policy statement, in order not to mislead the public.</p> <p>An organisation would not be required to provide a full copy of all data held at the time of the request, but would be entitled to first clean up the data by updating and removing irrelevant or dubious data. The organisation would then be obliged to provide the individual with a copy of all the remaining data.</p>