HIPSSA

Support for Harmonization of ICT Policies in Sub-Sahara Africa (HIPSSA)

DRAFT Southern African Development Community (SADC) MODEL LAW ON DATA PROTECTION

March 2011

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

The opinions expressed in this report are those of the author(s) and do not necessarily represent the views of the International Telecommunication Union (ITU) or its membership. The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Acknowledgements

Table of content

Preamble

Many institutions or international organizations consider data protection to be fundamental to the development of the individual in a democratic society and the construction of well-being. As such, data protection is a servant of the individual, both in the personal domain as well as in the workplace.

Owing to the connection between data protection and the protection of privacy, however, one must acknowledge a broader application for data protection. Indeed, several human rights are concerned including freedom of expression, freedom of association, etc. Data protection prevents the reliance on personal data for the differentiation between individuals based on, among other elements, religious beliefs, union affiliation, sex, race, filiation, and health-related data.

In addition to these considerations based on fundamental human rights, there is a real explosion of information and communication technologies that could affect this right to the protection of personal data in commercial activities as well as in electronic government (eGov) activities. The development of these technologies involves the proliferation of databases used to store and process much personal data. Then, the interconnection of these databases could lead to illegitimate tracing of individuals in their various private as well as professional activities. Furthermore, it can be seen that information and communication technologies are becoming increasingly important in decision made regarding individuals particularly in view of the information contained in the databases described above. Data protection regulation should seeks to ensure that the benefits of using information and communication technologies is not concurrent with weakened protection of personal data

This means that information must be correct, but also relevant to the purpose specified and declared. The principle of only collecting and processing the personal data necessary for a specified and declared purpose must be implemented. In addition, the controller (that is to say the person who determines the purpose or goal of processing and means that will be implemented) has an obligation to update the data and limit its collection and processing.

It also needs to ensure that data is not disclosed without permission of the individual or a legal provision. This implies the implementation of organizational and technical measures ensuring the safety of treatment involving, among others, the collection and storage of personal data.

This requirement implies a principle of accountability (principle of accountability) in charge of the data controller but also his/her data processor according to the sensitivity of the processed data. There are, in fact, data that are less sensitive than others, and which may require a lower standard of protection. For example, if a database contains only first and last names, the data are normally not sensitive and, therefore, generate less risk of intrusion or theft and less sophisticated security is required. However, a database of health-related personal data or data revealing race identity would require greater security.

As has been shown, two categories of data exist: sensitive data that can affect in itself an individual's privacy and data that is not sensitive. The first category reveals a person's religious affiliation, ethnic origin and health. This can also be genetic data which has the particularity to concern many people, namely those of the same family. So we need to define specific rules for this particular category of sensitive data but taking on account the fact that some sensitive data are not processed for what they content or reveal as the picture of someone hearing religious cloth on a website or in a directory. The data (picture) is not processed for the religious meaning but only for the picture of the person in the context of showing it on the website or in the directory. Therefore, the rules shall reflect this. However, this is not valid for genetic data, biometric data and data related to children, offences, criminal sentences or security measure which are highly sensitive data.

Concurrently it is necessary to provide to the individual control on his/her own data via a right of access from which will result, among others, a right of rectification and opposition. There may additionally be present the need to set up a system of sanctions to make the law fully effective. Indeed, a law without sanction is subject to violation that makes it totally ineffective.

In addition, it should be noted that with globalisation, traditional borders between regions and countries are becoming increasingly permeable. This implies that the personal data is subject to cross-border treatments more and more often. The States need to determine the rules that govern such transfers in order to only allow them under conditions that ensure personal data are protected. These rules of data protection will be more easily applicable if many countries adopt equivalent ones. This therefore leads to the texts adopted on a regional scale. It is indeed important that many countries adopt common set of rules to ensure effective protection of the right to protection of personal data. The objective of the proposed model law is to create a uniform system in a given area in order to create a safe environment for citizens.

The establishment of a uniform system of rules requires cooperation between countries to ensure continuity in the uniform. This cooperation can take place through the collaboration of the protection of personal data via an international working group.

Moreover, the protection regime of personal data must account for social and religious customs as well as on existing regional policies to achieve its goal of protection and harmonization. Existing tools such as the draft convention of the African Union on draft African union convention on the establishment of a credible legal framework for cyber security in Africa, the texts of Southern African Development Community (SADC), Economic Community Of West African States (ECOWAS) and existing national legislations including constitutional provisions.

The establishment of a protection regime for personal data will only be effective with the creation of a Protection Authority in order to foster compliance with the law and protection of privacy in general. This authority must also be endowed with regulatory powers in order to, for example, clarify certain principles of the model law.

It is with the above in mind that it is that it is acknowledged that the protection of personal data involves the establishment of a specific and adapted regime to the particularities of each region as set out in this Model Law.

Short Title

This legislation may be cited as the Data Protection Act, and shall come into force and effect [on xxx/ following publication in the *Gazette*].

Objective

The objective of data protection legislation in [insert name of country] shall be to combat the violations of data likely to arise from the collection, processing, transmission, storage and use of personal data.

Chapter 1. Definitions

Definitions

1. (1). **Code of conduct:** refers to the data-use charters drafted by the data controller in order to institute the rightful use of IT resources, the Internet, and electronic communications of the structure concerned, and which have been approved by the data protection authority.

(2). **Consent:** refers to any manifestation of specific, unequivocal, freely given, informed expression of will by which the data subject or his/her legal, judicial or legally appointed representative accepts that his/her personal data be processed.

(3). **Data:** refers to all representations of information notwithstanding format or medium .

(4). **Data controller or controller:** refers to any natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data. Where the purpose and means of processing are determined by or by virtue of an act, decree or ordinance, the controller is the natural person, legal person or public body has been designated as such by or by virtue of that act, decree or ordinance.

(5). **Data controller's representative or controller's representative:** refers to any natural person, legal person or public body permanently established on the territory [of the concerned country], who takes the place of the data controller in the accomplishment of the obligations set by the present model law.

(6). **Data processor:** refers to a natural person, legal person, or public body which processes personal data for and on behalf of the controller and under the data controller's instruction, except for the persons who, under the direct authority of the controller, are authorised to process the data.

(7). **Data protection officer or DPO**: refers to any individual appointed by the data controller charged with ensuring, in an independent

manner, compliance with the obligations provided for in this Model law except where a transfer of personal data to a State that is not a Member State of the SADC

(8). **Data subject:** refers to any individual who is the subject of the processing of personal data and who is identified or identifiable.

(9). **Identifiable person:** (a) is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

(b) To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person.

(10). **File:** (a) refers to any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

(b) It includes electronic or any other support.

(11). **Genetic data:** refers to any information stemming from a Deoxyribonucleic acid (DNA) analysis.

(12). **Health professional:** refers to any individual determined as such by the national law.

(13). **Child:** refers to any individual who is not of age or has not similar status according to his/her national law [or national law of the State implementing this model law].

(14). **Personal data:** refers to any data relating to a data subject.

(15). **Processing:** refers to any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as obtaining, recording or holding the data or carrying out any operation or set of operations on data, including –

(a) organization, adaptation or alteration of the data;
(b) retrieval, consultation or use of the data; or
(c) alignment, combination, blocking, erasure or destruction of the data.

(16). **Protection Authority or Authority:** refers to an independent administrative authority responsible for ensuring that personal data is processed in compliance with the provisions of this Model law. This implies a decision-making power independent of any direct or

indirect external influence on the Authority.

(17). **Recipient:** is natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular legal inquiry shall not be regarded as recipients

(18). **Register:** means the register referred to in chapter 3.

(19). **Sensitive data:** (a) refers to genetic data, data related to children, data related to offences, criminal sentences or security measure, biometric data as well as, if they are processed for what they reveal or contain, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, filiation, trade-union membership, the gender and the processing of data concerning health or sex life.

(b) refers also to any personal data which are considered by a Member State as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination.

(20). **Third party:** refers to any natural or legal person, un-associated organization or public authority other than the data subject, the controller, the processor and anyone who, under the direct authority of the controller or the processor, is authorized to process the data.

(21). **Transborder flow:** refers to any international flows of personal data by the means of electronic transmission or any other transmission means including data transmission by satellite.

(22). **Whistleblowing:** refers to legal system allowing individuals to report the behaviour of a member of their organization which, they consider contrary to a law or regulation or fundamental rules established by their organization.

Chapter 2. Scope of application

Scope of Application 2.

(1). This model law is applicable to any processing of personal data performed wholly or partly by automated means, and to the processing of personal data otherwise than by automated means which forms part of a filing system or is intended to form part of a filing system.

(2). This model law is applicable:

(a) to the processing of personal data carried out in the context of the effective and actual activities of any controller permanently established on [given country] territory or in a place where [given country] law applies by virtue of international public law;
(b) to the processing of personal data by a controller who is not permanently established on [given country] territory, if the means used, which can be automatic or other means located on [given country] territory, are not the same as the means used for processing personal data only for the purposes of transit of personal data through [given country] territory.

(3). In the circumstances referred to in the previous paragraph under (2)b, the controller shall designate a representative established on [given country] territory, without prejudice to legal proceedings that may be brought against the controller.

(4). This model law does not apply to the processing of personal data by a natural person in the course of purely personal or household activities.

(5). This model law cannot restrict:

(a) the ways of production of information which are available according to a national law or as permitted in the rules that govern legal proceedings;
(b) the power of the judiciary to constrain a witness to testify produce evidence.

Chapter 3. Data Protection Authority

Status and composition

3. (1). An independent and administrative authority called the Protection Authority or Authority is established and will be in charge of the control of the respect of this model law and the privacy on the national territory.

This implies a decision-making power independent of any direct or indirect external influence on the Authority.

(2). The Authority will be composed of judges appointed by his or her peers, a representative of [the Prime Minister or Head of the State], deputies appointed by their peers, people appointed by national organizations acting in the matter of fundamental human rights or non-governmental organizations, people appointed by national organizations acting in the matter of information and communication technologies. They are permanent members.

(3). The Authority will also include substitute members with the same distribution of professional backgrounds who will replace a permanent member when he/she is excused, absent or when his/her mandate becomes vacant.

(4). All members, permanent and substitute, shall have competencies in personal data protection, privacy or communication and information technologies.

(5). To be appointed as member, permanent or substitute, the candidates must fulfil the following conditions:

(a) They have the nationality of the country.
(b) They are in full possession of their civil and political rights.
(c) They are not a member of an organ of SADC or the parliament except for the members of Parliament appointed to be members of the Authority pursuant previous paragraph (2).

[The Member State shall establish specific rules related to the incompatibility between the function of members of the Authority and other functions as specific rules in order to avoid any conflicts of interest occurring before or during the mandate of the members of the Authority.]

(6). The members of the Authority are not allowed to attend any deliberations on matters in which they or their family members to the fourth degree have a personal interest.

(7). The members of the Authority are submitted to the obligation of secrecy according to the legal rules (such as the penal code).

(8). The members of the Authority are appointed for a term of […] years renewable […] time(s).

(9). The members can be removed from their function by the organ or organization that appointed them in the event of a breach of their duties stipulated in this model law or an offence to the integrity of their function.

(10). The members of the Authority benefit from immunity for the opinions they express in the execution of their function. The members cannot be removed from their function in relation to the opinions expressed or their acts fulfilled in their function as members.

(11). In the exercise of their function, the members shall remain

independent from the influence of instruction of any other public authority.

(12). The Authority's deliberations shall be legitimate when at least a majority of its members is present during its meetings. The decisions shall be taken by absolute majority. In the case of a tie, the President of the Authority, or, in his/her absence, his/her substitute shall have casting vote.

(13). Unless Article 5 (1) (c), all personnel, consultants and contractors to the Authority shall submit to the obligation of secrecy according to the legal rules (such as penal code) for the purpose of maintaining the confidentiality of all the facts, acts and information that may become known to such person(s)by their function.

(14). The President of the Authority shall be a judge with at least 5 years standing as such and shall have a dedicated full time appointment with the Authority. During his/her mandate, he/she cannot have any other professional activity. His/her salary is equal to that provided for someone occupying the post of [….], including pay rises and other employee benefits.

(15). Prior to carrying out their mandates, the President of the Authority and members, permanent and substitute, take the following oath administered by the Parliament:

"I swear to fulfil the duties of my mission conscientiously and impartially."

Powers

4. (1). The Authority:

(a) Shall be chiefly engaged in procuring that the controller's processing of personal data is compliant with this model law.

(b) shall issue its opinion either of its own accord, or at the request of the Government, the Parliament, on any matter relating to the application of the fundamental principles of the protection of privacy, in the context of this model law and any act containing provisions relating to the protection of privacy in relation to the processing of personal data.

(c) may submit to the Court any legislative or administrative act which is not compliant with the fundamental principles of the protection of the privacy in the framework of this model law as well as any law containing provisions regarding the protection of privacy in relation to the processing of personal data.

(d) may issue regulations in accordance with its powers under this model law which shall be exercisable by statutory instrument having force of law, which (except in the case of the initial regulations) shall be subject to annulment in pursuance of a resolution of the Parliament by a majority of 2/3 of the members of the Parliament.

(e) (i)may conduct inquiries either of its own accord or at the request of the data subject or any interested person, and in relation thereto may call upon the assistance of experts to carry out its functions i.e.it may instruct one or more of its members, accompanied by an expert if necessary, to carry out on-site investigations.

(ii) may demand, among other things, the disclosure of any documents that may be of use for their investigation.

(iii) shall have access to all places reasonably suspected to be the location for activities relating to the application of this model law.

(f) receives, by post or electronic means or any another equivalent means, the complaints lodged against a personal data processing and give feed-back to the claimants.

(g) receives, by post or electronic means or any another equivalent means, the complaints lodged in the exercise of the rights of the data subject pursuant chapter 7 of this model law.

(h) May conduct frequent consultation with major stakeholders (as such as Parliament, relevant ministry, general public) on matter appearing necessary for securing effective data protection for any such services, facilities, apparatus or directories under this model law.

Duties

5. (1). The Authority shall:

(a) answer to any request of opinion regarding the protection of

privacy in relation to the processing of personal data;

(b) receive the notification of processing pursuant to Article 26 (1) and enforce its compliance with this model law.

(c) unless otherwise described by law, shall, without delay, inform the judicial authority of any offence it is aware of and considers necessary to bring to the knowledge of the judicial authority.

(2). pronounce administrative sanctions such as the cancelling of the authorization of processing, fines or awarding of damages to the benefit of the injured data subject in the case of violation of the provisions of this model law.

(3). provide the authorization pursuant Article 28;

(4). create, maintain and update the register which shall be accessible to any person who requests access without any motivation

(5). receive notification(s) of security breaches set out in Article 25;

(6). receive and give the authorization for draft, modification or extension of the codes of conduct set in chapter 12

(7). provide opinion on how legal data protection legal framework can be simplified and improved;

(8). set mechanisms of cooperation with protection authorities from third countries, if any, and mainly to resolve possible cross-border dispute under this Model law where the dispute lies within the competence of national data protection authority from more than one Member State;

(9). participate in any international negotiation on matters of data protection;

(10). submit, once a year, an activity report to be presented to the institution to which the Authority reports;

6. (1). The Authority may apply for a Court order for the expeditious preservation of data, including traffic data, where it has reasonable grounds to believe that such data is vulnerable to loss or modification.

(2). Where the Court is satisfied that an order may be made under previous Paragraph (1), it shall issue a preservation order specifying a period which shall be not more than 90 days during which the order shall remain in force.

(3). The Court may, on application made by the Authority, extend the period specified in previous Paragraph (2) for such time as the judge thinks fit.

7. (1). The Authority must draw up its rules of procedure within a […] term following its establishment. These rules shall be published.

(2). These rules set the proceedings for:

(a) The deliberations, instruction and presentation of the cases;
(b) The complaint, inquiry and sanction;
(c) All other proceeding set in this chapter.

(3). The Authority' deliberations are only legitimate when at least a majority of members is present during its meetings. It takes decisions by absolute majority. In case of a tie, the President of the Authority, or in his/her absence his/her substitute, has the casting vote.

Access to the Authority

8. (1). Any person proving his/her identity has the right to address the Authority, free of charge, by himself/herself or by his/her lawyer or any other individual or legal body duly appointed.

Sanctions

9. (1). The Authority may impose the following:

(a) a warning to a data controller failing to comply with the obligations of this model law.

Such warning shall be regarded as a sanction.

or

(b) a formal notice to comply on said data controller to cease the non-compliance within a given deadline. In case of urgency, this deadline may be limited to five days.

(2). Should the controller fail to comply with the notice served, the Authority may pronounce the following sanctions, after due hearing of the parties:

(a) Limitation or ceasing of the processing or suspension of authorization, for a maximum period of three months;

and/or

(b) Financial penalty of (…);

(3). In case of serious and immediate violation of the individual rights and liberties, the Authority may rule, in summary proceedings:

(a) the limitation or ceasing of the personal data processing;

or

(b) the temporary or definitive access to some personal data processed;

or

(c) the temporary or definitive processing not compliant with the provisions of this model law.

(4). The sanctions and decisions taken by the Authority may be subject to appeal through the judicial authorities.

Financing

10. (1). For the accomplishment of its mission, the Authority shall receive a grant from the Parliament which ensures its capability to exercises its duties and powers.

(2). The Authority will collect the financial sanction pronounced against data controllers pursuant this model law.

(3). The Authority shall present an annual report to the institution to which the Authority reports.

Chapter 4. Quality of the data

Quality of the data

11. (1). The data controller shall ensure that personal data processed is:

(a) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;

(b) accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that data which is inaccurate or incomplete with respect to the purposes for which it is collected or for which it is further processed, is erased or rectified;

(c) retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed. The Authority shall establish appropriate safeguards for personal data retained longer than permitted above for historical, statistical or scientific research purposes.

(2). The data controller shall take all appropriate measures to ensure that personal data processed can be exploited regardless of the support used and ensure that the evolution of technology will not be an obstacle to the operation.

(3). The controller ensures compliance with the rules laid down in Paragraphs (1) and (2) by any person working under his/her authority or any subcontractor.

Chapter 5. General rules on the processing of personal data

Generality

12. (1). The data controller shall ensure that the processing of personal data is necessary and that the personal data is processed fairly and lawfully

Purpose

13. (1). The data controller shall ensure that personal data is collected for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions, that is not further processed in a way incompatible with those purposes.

(2). Under the conditions established by the Authority, further processing of data for historical, statistical or scientific research purposes is not considered incompatible.

Non-sensitive data

14. (1). The processing of non-sensitive personal data is permitted, without the consent of the data subject, if necessary:

(a) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

or

(b) for compliance with an obligation to which the controller is subject by or by virtue of a law;

or

(c) in order to protect the vital interests of the data subject;

or

(d) for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller or in a third party to whom the data is disclosed;

or

(e) for the promotion of the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this model law.

(2). The Authority can specify the circumstances in which the condition stipulated under e) is considered as not having been met.

Sensitive data

15. (1). (a) The processing of personal data, if they are processed for what they reveal or contain, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, filiation, trade-union membership, the gender and the processing of data concerning sex life as well as any personal data which are considered by a Member State as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination, is prohibited unless the data subject has given his/her consent in writing for such processing of personal data, unless the law states that the prohibition cannot be lifted by the written consent of the data subject.

(b) This consent can be withdrawn by the data subject at any time and without any explanation and is free of charge.

(c) The Authority may determine the cases in which the prohibition to process the data referred to in this article cannot be lifted even with the data subject's consent.

(2). Paragraph (1) above shall not apply where:

(a) the processing is necessary to carry out the obligations and specific rights of the controller in the field of employment law; or
(b) the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his/her consent or is not represented by his/her legal, judicial or agreed representative; or
(c) the processing is carried out in the course of its legitimate activities by a foundation, association or any other non-profit organization with a political, philosophical, religious, health-insurance or trade-union aim and on condition that the processing relates solely to the members of the organization or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to a third party without the data subjects' consent; or
(d) the processing is necessary to comply with social security laws; or
(e) the processing is necessary, with appropriate guaranties, for the establishment, exercise or defense of legal claims; or
(f) the processing relates to data which has apparently been made public by the data subject; or
(g) (i) the processing is necessary for the purposes of scientific research.

(ii)The Authority shall be entitled to specify the conditions under which such processing may be carried out.

or

(h) the processing is carried out according to the legislation on public statistics; or
(i) the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment to the data subject or one of his/her relatives, or the

management of health-care services provided in the interest of the data subject, and when the data is processed under the supervision of a health professional; or

(j) the processing of personal data referred is authorized by a law or any equivalent legislative act for another reason of substantial public interest; or

(k) the processing is carried out by associations with a legal personality or organizations of public interest whose main objective is the protection and promotion of human rights and fundamental freedoms, with a view to achieving that objective, provided that the processing has been authorized by the Authority;

(3). (a) The processing of personal data referred in Paragraph 2 (i) above. except where the data subject provides written consent or when the processing is necessary for preventing of an imminent danger or the mitigation of a specific criminal offence, can only be done under the authority of a health professional.

(b) In this case, the health professional and his/her agents are subject to the duty of secrecy.

(4). (a) Without prejudice to the application of Articles 16 to 19, the processing of personal data relating to sex life is authorized if it is carried out by an association with a legal personality or by an organization of public interest whose main objective, according to its articles of association, is the evaluation, guidance and treatment of persons whose sexual conduct can be qualified as an offence, and who has been recognized and subsidized for the achievement of that objective by the competent public body; for such processing, the objective of which must consist of the evaluation, guidance and treatment of the persons referred to in this paragraph, and for which the processing of personal data, if it concerns sex life, only relates to the aforementioned persons, the competent public body must grant a specific, individualized authorization, having received the opinion of the Authority.

(b) The authorization referred to in this paragraph specifies the duration of the authorization, the conditions for supervision of the authorized association or organization by the competent public body, and the way in which the processing must be reported to the Authority.

16. (1). (a) The processing of genetic data, biometric data and health data if it is processed for what it reveals or contains, is prohibited unless the data subject has given his consent in writing to the processing of the above mentioned data except if the law states that the prohibition cannot be lifted even with the written consent of the data subject.

(b) The consent referred to in previous paragraph (a) can be withdrawn by the data subject at any time without any motivation and free of charge;

(c) The Authority may determine the cases in which the prohibition to process the data referred to in this article cannot be lifted by the data subject's consent.

(2). Previous Paragraph (1) shall not apply where:

(a) the processing is necessary to carry out the specific obligations and rights of the controller in the field of employment law; or
(b) the processing is necessary to comply with social security laws; or
(c) the processing is necessary for the promotion and protection of public health, including medical examination of the population; or
(d) the processing is required by or by virtue of a law or any equivalent legislative act for reasons of substantial public interest; or
(e) the processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving his/her consent or is not represented by his/her legal, judicial or agreed representative; or
(f) the processing is necessary for the prevention of imminent danger or the mitigation of a specific criminal offence; or
(g) the processing relates to data which has apparently been made public by the data subject; or
(h) the processing is necessary for the establishment, exercise or defense of legal rights; or
(i) (i)the processing is required for the purposes of scientific research.

(ii) The Authority establishes the conditions to which such processing must answer.

or

(j) the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment for the data subject or to one of his/her relatives [to be determined by the given State], or the management of health-care services in the interest of the data subject, and the data is processed under the supervision of an health professional;

(3). (a) Health-related personal data may only be processed under the responsibility of a health-care professional, except if the data subject has

given his/her written consent or if the processing is necessary for the prevention of imminent danger or for the mitigation of a specific criminal offence.

(b) Health-related personal data must be collected from the data subject.

(4). The Authority shall be entitled to specify the conditions under which such processing may be carried out.

(5). It may only be collected from other sources if paragraphs (3) and (4) above are complied with, and if such is necessary for the purposes of the processing, or if the data subject is incapable of providing the data.

(6). When the processing affected by this article, the health professional and his/her agents are subject to the duty of secrecy.

17. (1). In the scope of articles 15 (2) (i) and 16 (2) (c) and 16 (2) (j), the processing of genetic data and, if they are processed for what they reveal or contain, personal data concerning health can be processed only if a unique patient identifier is given to the patient, which has to be different from any other identification number, by the public authority set by the law for this purpose.

(2). The interconnectivity of this unique patient identifier with any other identifier which can allow the data subject in the sense of the Article 1 (9) will be possible only by the authorization of the Authority.

18. (1). The processing of personal data relating to litigation that has been submitted to courts and tribunals as well as to administrative judicial bodies, relating to suspicions, prosecutions or convictions in matters of crime, administrative sanctions or security measures, is prohibited, except if the processing is done:

(a) under the supervision of a public body or ministerial civil servant as defined by the law [of the given State] and if the processing is necessary for the fulfillment of their duties; or
(b) by other persons, if the processing is necessary to achieve purposes that have been established by law; or
(c) by natural persons, private or public legal persons, to the extent that the processing is necessary to manage their litigations; or
(d) by lawyers or other legal advisors, to the extent that the processing is necessary for the protection of their clients' interests; or
(e) if the processing done is necessary to scientific research. The Authority establishes the conditions which have to be followed for such processing.

(2). Persons authorized under this article to process such personal data are subject to an obligation of secrecy.

(3). The Authority shall establish the specific conditions to be met when processing the personal data referred in this article.

19. The personal data of the child will be processed only in respect of the rules of representation pursuant Article 37.

20. (1). The Authority can set exceptions to the present chapter, at Article 21 and 22 and Chapter 7 when the processing is conducted by any person lagally subject to an obligation of secrecy due to the nature of their office.
(2). The paragraph (1) above is not applicable to the client/patient of a person to whom such an exception applies.

Chapter 6. Duties of the data controller and data processor

Information

21. (1). When personal data relating to the data subject is obtained directly from the data subject, the controller or his/her representative shall concurrently provide the data subject with at least the following information, unless the data subject has already received such information:

(a) the name and address of the controller and of his/her representative, if any;
(b) the purposes of the processing;
(c) the existence of the right to object, by request and free of charge, to the intended processing of personal data relating to him/her, if it is obtained for the purposes of direct marketing;
(d) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;
(e) taking in account the specific circumstances in which the data is collected, any complementary information, if it is necessary to ensure a fair processing for the data subject, such as:

(i) the recipients or categories of recipients of the data;

(ii)whether it is compulsory to reply, and what the possible consequences of the failure to reply are;

(iii) the existence of the right to access and rectify the personal data relating to him/her; except where such additional information, taking into account the specific circumstances in which the data is collected, is not necessary to guarantee correct processing with respect to the data subject.

(f) other information dependent on the specific nature of the processing, as specified by the Authority.

22. (1). When the personal data is not collected from the data subject himself/herself, the controller or his/her representative must provide the data subject with at least the information below when recording the personal data or when considering communication to a third party, and at the very latest when the data is first disclosed, unless the data subject has already received such information:

(a) the name and address of the controller and of his/her representative, if any;
(b) the purposes of the processing;
(c) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;

(d) the existence of a right to object, by request and free of charge, to the intended processing of personal data relating to him/her, if it is obtained for the purposes of direct marketing; in that case, the data subject must be informed prior to the first disclosure of the personal data to a third party or prior to the first use of the data for the purposes of direct marketing on behalf of third parties;

(e) Taking in account the specific circumstances in which the data is collected, any complementary information, if they are necessary to ensure a fair processing for the data subject, such as:

(i) the categories of data concerned,

(ii) the recipients or categories of recipients of the data,

(iii) the existence of the right to access and rectify the personal data relating to him/her, unless such additional information, taking into account the specific circumstances in which the data is provided, is not necessary to guarantee fair processing with respect to the data subject.

(f) other information dependent on the specific nature of the processing, which is specified by the Authority.

(2). Previous paragraph (1) is not applicable if:

(a) informing the data subject proves impossible or would involve a disproportionate effort, in particular for data collected for statistical purposes or for the purpose of historical or scientific research, or for the purpose of medical examination of the population with a view to protecting and promoting public health;

or

(b) if personal data is recorded or provided with a view to the application of a provision laid down by or by virtue of an act, decree or ordinance.

(3). The Authority shall establish the conditions for the application of this Paragraph.

Authority to process

23. Any person having access to the personal data and acting under the authority of the controller or of the processor, as well as the processor himself/herself, may process personal data only as instructed by the controller, without prejudice to any duty imposed by law.

Security

24. (1). (a) In order to safeguard the security of the personal data, the controller or his/her representative, if any, as well as the processor, must take the appropriate technical and organizational measures that are necessary to protect the personal data from negligent or unauthorized destruction, negligent loss, as well as from alteration, access and any other unauthorized processing of the personal data.

(b) These measures must ensure an appropriate level of security taking into account the state of technological development in this field and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks on the other.

(c) The Authority may issue appropriate standards relating to information security for all or certain categories of processing.

(2). The data controller and his/her data processor, if there is any processing done for him/her, must choose a data processor who gives enough guarantees regarding the technical and organizational security measures concerning the processing to be done and must ensure the respect of these measures.

(3). (a) Any recourse to data processor must be governed by a contract or any other legal act which links the data processor to the data controller.

(b) The contract or legislative act must set:

(i) that the data processor acts only under instruction of the data controller;

(ii) that the data processor is also responsible for discharging the duties set out in previous paragraph (1).

25. (1). The data controller or his/her representative must notify the Authority, without any undue delay, of any security breach affecting personal data.

(2). The data processor must notify the data controller, without undue delay, of any security breach affecting personal data he/she processes on behalf of the data controller.

Obligation of notification to the Authority

26. (1). (a) Prior to any wholly or partly automated operation or set of operations intended to serve a single purpose or several related purposes, the controller or his/her representative, if any, must notify the Authority.

(b)Any modification to the information given according Article 27 must be notified the Authority.

(2). Previous Paragraph (1) does not apply to operations having the sole purpose of keeping a register that is intended to provide information to the public by virtue of an act, decree or ordinance and that is open to consultation either by the general public or by any person demonstrating a legitimate interest.

(3). The Authority can exempt certain categories from notification under this article if:

(a) taking into account the data being processed, there is no apparent risk of infringement of the data subjects' rights and freedoms, and if the purposes of the processing, the categories of data being processed, the categories of data subjects, the categories of recipients and the data retention period are specified.

(b) (i)The data controller has appointed a data protection officer.

(ii) The appointment of the data protection officer shall be notified to the Authority.

(iii) The data protection officer shall:

- be a person who shall have the qualifications required to perform his/her duties;
- keep a list of the processing carried out, which is immediately accessible to any person applying for access, and may not be sanctioned by his/her employer as a result of performing his/her duties.

(iv) He/she may apply to the Authority when he/she encounters difficulties in the performance of his/her duties.

(v) In case of non-compliance with the provisions of this model law, the Authority shall order the data controller to carry out the formalities provided for in previous paragraph (1).

(vi) In case of breach of his/her duties, the representative shall be discharged from his/her functions upon the demand, or after consultation, of the Authority.

(vii) The Authority establishes the specific rules establishing the function of data protection officer.

(4). If exemption from the duty of notification has been granted for automatic processing in accordance with the previous paragraph, the data controller must disclose the items of information mentioned in Articles 27 to any person requesting them.

(5). The processing performed by the public authorities cannot benefit from the exception of notification set by paragraph (3).

Content of the notification

27. (1). The notification must state, at least,:

(a) the date of notification and the act, decree, ordinance or regulatory instrument permitting the automatic processing, if any;
(b) the surname, first names and complete address or the name and registered offices of the controller and of his/her representative, if any;
(c) the denomination of the automatic processing;
(d) the purpose or the set of related purposes of the automatic processing;
(e) the categories of personal data being processed and a detailed description of the data referred to in articles 7 to 11;
(f) a description of the category or categories of the data subjects;
(g) the safeguards that must be linked to the disclosure of the data to third parties;
(h) the manner in which the data subjects are informed, the service providing for the exercise of the right to access and the measures taken to facilitate the exercise of that right;
(i) the interconnectivities planned or any other form of linking with other processing;
(j) the period of time after the expiration of which the data may no longer be stored, used or disclosed;
(k) a general description containing a preliminary assessment of whether the security measures taken pursuant to Chapter 6, section 3 above are adequate;
(l) the recourse to a data processor;
(m) the transfers of data to a third country as planned by the data controller;

(2). The Authority may establish other information which must be mentioned in the notification.

(3). Where the Authority is of the opinion that the processing or transfer of data by a data controller entails specific risks to the privacy rights of data subjects, he may inspect and assess the security measures prior to the beginning of the processing or transfer.

(4). The Authority may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a data controller.

Authorization

28. (1). The Authority establishes the categories of processing which represent some specific risks towards the fundamental rights of the data subject and which request an authorization from the Authority.

(2). Such authorization is given after reception of the notification from the data controller or from the data protection officer who, in case of doubt, must seek advice from the Authority.

Openness of the processing

29. (1). (a) The Authority shall keep a register of all automatic processing operations of personal data.

(b) Any entry in the register must include the information mentioned in Article 27.

(c) The register shall be open to consultation by all members of the public, in the manner determined by the Authority.

(2). In case of the processing exempted from notification by this model law, the Authority may, either by virtue of its office or at the data subject's request, impose upon the controller the obligation to disclose to the data subject all or part of the information mentioned in Article 27.

Accountability

30. (1). The data controller shall:

(a) take all the necessary measures to observe the principles and obligations set out in this model law including chapters 4 and 5.

and

(b) have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the Authority in the exercise of its powers.

Chapter 7. Rights of the data subject

Right of access

31. (1). Any data subject who proves his/her identity has the right to obtain, without any explanation and free of charge, from the controller or his/her representative, if any:

(a) information on whether or not data relating to him/her is being processed, as well as information regarding the purposes of the processing, the categories of data the processing relates to, and the categories of recipients the data is disclosed to

(b) communication of the data being processed in an intelligible form, as well as of any available source of information;

(c) information about the basic logic involved in any automatic processing of data relating to him/her in case of automated decision making;

(d) information regarding his/her right of complaint under this chapter and his/her right to consult the register referred to in article 29 if necessary.

(2). (a) To obtain such information the data subject shall submit a signed and dated request to the controller or data protection officer.

(b) The Authority shall be entitled to specify further conditions for the application of this paragraph (2) (a).

(3). (a) When the sensitive personal data is processed with a purpose of scientific research and there is no evident risk of infringing on the data subject's right to protection of his/her privacy and the data is not used in order to take measures and decisions with regard to an individual, informing the data subject may be postponed at the latest until the moment the research is ended, but only to the extent that informing the data subject would seriously compromise the research.

(b) In this case the data subject must have given to the data controller his/her previous written consent to the processing of personal data relating to him/her for scientific research purposes and to postponing, for that reason, the moment at which he is informed.

(4). The waive of any charge pursuant to Paragraph (1) above may be refused by the data controller in case of misuse of request by the data subject.

(5). The data controller's decision may be the subject of a complaint by the data subject to the Authority in accordance with Article 4.

Right of rectification, deletion and temporary limitation of access

32. (1). (a) The data subject has the right, as the case may be and free of charge, of rectification, deletion of the personal data relating to him/her or temporary limitation of access to these personal data if the processing is not compliant with this model law, especially if the personal data are not complete or not accurate.

(b) Any person also has the right to obtain free of charge the deletion of or the prohibition to use all personal data relating to him/her that is incomplete or irrelevant with a view to the purpose of the processing, or where the recording, disclosure or storage of the data is prohibited, or where it has been stored for longer than the authorized period of time.

(2). The data subject has the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, deletion or temporary limitation pursuant to paragraph (1) unless this proves impossible or involves a disproportionate effort.

(3). The free of charge pursuant paragraph (1) may be refused by the data controller in the case of misuse of the request by the data subject.

(4). The data controller's decision may be the subject of a complaint by the data subject to the Authority in accordance with Article 6.

Right of objection

33. (1). The data subject has the right:

(a) (i) to object at any time and free of charge, on compelling legitimate grounds relating to his/her particular situation (such as judicial proceeding), to the processing of data relating to him/her, unless the lawfulness of the processing is based on the reasons referred to in Articles 14 (1) (a), 14 (1) (b), 15 (2) (a), 15 (2) (d), 15 (2) (j), 16 (2) (a), 16 (2) (b) and 17 (2) (d).

(ii) Where there is a justified objection, the processing in question may no longer involve those data;

or

(b) to be informed before personal data are disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or use.

(2). The waiver of any charge pursuant to paragraph (1) may be refused by the controller in the case of misuse of the request by the data subject.

(3). The data controller's decision may be the subject of a complaint by the data subject to the Authority in accordance with Article 6.

Delays

34. The data controller must give an answer to the request of the data subject within 45 days. If not, a complaint may be addressed to the Authority.

Power to make regulation

35. The Authority can specify further rules relating to the exercise of the right referred to in Articles 31 to 33.

Decision taken purely on the basis of automatic data processing

36. (1). A decision having legal effects on a person or significantly affecting him/her, must not be taken purely on the basis of automatic data processing with the aim of assessing certain aspects of his/her personality.

(2). The prohibition referred to in paragraph (1) is not applicable if the decision is taken in the context of an agreement or is based on a provision established by or by virtue of law. That agreement or provision must contain suitable measures to safeguard the legitimate interests of the data subject defined by his/her national law or international convention. The latter must be given at least the chance to defend his/her point of view efficiently.

Representation of the data subject

37. (1). If the data subject is a child, his/her rights pursuant this model law may be exercised by his/her parents or legal guardian unless the law states that the child may act by himself without being represented by his/her parents or legal guardian.

(2). Following his/her age and capability, he/she may be associated to the exercise of his/her rights.

38. (1). (a) When the data subject not subject to Article 37, is physically, mentally (both must be attested by a physician or any authority or person legally competent) or legally incapable of exercising the rights given by this model law, these rights are exercised by the spouse, the partner who cohabites with the data subject.

(b) If this person doesn't want to accept the charge or if he/she is in default, the rights are exercised, in subsequent sequence, by a child who is of age, a parent, a brother or sister who is of age of the data subject.

(2). (a) If such person doesn't accept the charge or is in default, a specific guardian designed by the competent Court will exercise the rights of the data subject.

(b) This is also valid in case of conflict between two or more people mentioned in paragraph 1.

(3). The data subject is associated to the exercise of his/her rights as much as possible taking in account his/her capability.

Chapter 8. Recourse to the judicial authority

Recourse to the judicial authority

39. Subject to the exhaustion of the appeal offered through the Authority under this law, the data subject shall be entitled to pursue legal appeals with the relevant judicial authorities.

40. The law maker shall set up a class action system to assist of the data subject in the exercise of their rights set up under this model law.

Chapter 9. Sanctions

Sanctions

41. (1). Any member, permanent of substitute, personnel, consultant, contractor or other member of staff of the Authority or any expert who has violated the obligation of secrecy referred to this model law shall be liable for the payment of a fine of (…).

(2). Any data controller, his/her representative, agent or assignee who does not comply with the obligations laid down in Articles 24 to 25, shall be punished with a fine of (…).

(3). A fine of (…) to (…) shall be imposed on:

(a) any controller, his/her representative, agent or assignee processing personal data in violation of the conditions imposed by Articles 11 (1), 12 and 13;
(b) any controller, his/her representative, agent or assignee processing personal data in cases other than those in Article 14;
(c) any controller, his/her representative, agent or assignee processing personal data in violation of Articles 15 to 19;
(d) any controller, his/her representative, agent or assignee having failed to communicate the information referred to in article 31 (1) within (…) days of receipt of the request, or who knowingly communicates incorrect or incomplete information;
(e) any person who resorts to acts of violence, force, threats, donations or promises with the purpose of forcing another person into disclosing information that was obtained through the exercise of the right defined in Article 31 (1), or with the purpose of obtaining the other person's consent for the processing of personal data relating to that person;
(f) any controller, his/her representative, agent or assignee having started, managed, continued to manage or terminated the automatic processing of personal data without meeting the requirements of Article 26;
(g) any controller, his/her representative, agent or assignee having communicated incomplete or incorrect information in the notifications imposed by Article 27;
(h) any controller, his/her representative, agent or assignee who, in violation of article 29 (2), refuses to communicate to the Authority information requested;
(i) any person who transfers personal data or has personal data transferred to a country outside the SADC included in the list referred to in Article 44 (2), or any person who authorizes such transfers despite the requirements of Article 45;
(j) any person who prevents the Authority, its members or its experts from proceeding with the inquiry referred to in Article 4.

(4). Upon conviction for any of the offences described in this article, the Court shall order the entire or partial publication of the judgment in one or more newspapers in the manner it shall determine, and at the expense of the convicted person.

(5). (a) Upon conviction for any of the offences described in this article, the judge can pronounce the seizure of the media containing the personal data to which the offence relates, such as manual filing systems, magnetic discs or magnetic tapes, except for computers or any other equipment, or he can order the deletion of the data.

(b) Seizure or deletion can also be ordered even if the media containing the personal data do not belong to the person convicted.

(c) The objects seized shall be destroyed when the judgment has become final.

(6). The present article is not an impeachment to any measure of leniency set by law as the suspension or the suspended sentence except for the sentences set in Paragraphs (4) and (5) above.

(7). Without prejudice to the revocation of competences laid down in particular provisions, the Court can, upon conviction for an offence mentioned in this article, impose a prohibition to manage any processing of personal data, directly or through an intermediary, for a maximum of […] years.

(8). Any violation of the prohibition laid down in paragraph 7 above or any recidivism relating to the offences referred to in this article, shall be punished with a […]-month to […]-year imprisonment and/or with a fine of […] to […].

(9). The controller or his representative shall be liable for the payment of the fines incurred by his agent or assignee

Chapter 10. Limitations

Limitations

42. (1). The Member States can take provisions to limit the obligations and rights pursuant Articles 11 (1), 12 and 13, Articles 21 and 22, Articles 31, 32 and 33 when such limitation is necessary to preserve:

(a) State security;
(b) defence;
(c) public safety (including the economic well-being or interest of the State when the processing operation relates to State security matters);
(d) the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures or violation to professional codes of conduct in the case of a regaled profession.
(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (c) and (d).

(2). (a) Article 11 (1) (c), Articles 15, 18, 21, 22, 26, 31 and 32 and Chapter 11 shall not apply to processing of personal data carried out for the sole purpose of:

- literary and artistic expression;

and

- professional journalism, according to the ethical rules of this profession.

(b) However, for processing mentioned in Paragraph (2) above, the exemption from the obligation to make a declaration as provided for in Article 26 is conditional on the appointment, by the data controller, of an data protection officer who belongs to a media undertaking, who maintains a register of processing carried out by the data controller and who independently ensures the proper application of the provisions of this model law. This appointment shall be notified to the Authority according to Article 26.

(c) In the event of non-compliance with the provisions of this model law that apply to the processing provided for in this article, the data controller shall be ordered by the Authority to bring matters into conformity with this model law. In the event of a failure to perform his/her duties, the officer is discharged from his/her functions at the request of or after consultation with the Authority.

(3). The provisions of the previous paragraphs shall not prevent the application of the provisions of the [for example, the Civil Code], the laws relating to the media and the Criminal Code that provide for the conditions of the exercise of the right of reply and that prevent, limit,

compensate and, if necessary, sanction violations of privacy and attacks on the reputation of individuals.

Chapter 11. Transborder flow

To a Member State which transposed this model law

43. (1). Without prejudice to Articles 11, 12, 13 and 17, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of this model law,

(a) 1. if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public body, or

(b) (i) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

(ii) The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient.

(iii) The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified.

(c) The recipient shall process the personal data only for the purposes for which they were transmitted

To a Member state which didn't transposed this model law or to a non Member State

44. (1). (a) Personal data shall only be transferred to recipients, other than Member States of the SADC, which are not subject to national law adopted pursuant to this model law, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organization and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.

(b) The adequacy of the level of protection afforded by the third country or international organization in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organization, the rules of law, both general and sectorial, in force in the third country or international organization in question and the professional rules and security measures which are complied with in that third country or international organization.

(2). The Authority shall lay down the categories of processing operations for which and the circumstances in which the transfer of personal data to countries outside the SADC is not authorized.

45. (1). By way of derogation from Article 46, a transfer or a set of transfers of personal data to a country outside the SADC which does not ensure an

adequate level of protection may take place in one of the following cases:

(a) the data subject has unambiguously given his/her consent to the proposed transfer;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;
(e) the transfer is necessary in order to protect the vital interests of the data subject;
(f) the transfer is made from a register which, according to acts or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.

(2). Without prejudice to the provisions of the previous paragraph, the Authority may authorize a transfer or a set of transfers of personal data to a country outside the SADC which does not ensure an adequate level of protection, if the controller ensures adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, and regarding the exercise of the corresponding rights; such safeguards can result from appropriate contractual clauses in particular.

Chapter 12. Code of conduct

Code of Conduct

46. (1). This model law encourages the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant this model law, taking account of the specific features of the various sectors.

(2). Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the Authority.

(3). Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this model law. If it sees fit, the authority shall seek the views of data subjects or their representatives.

Chapter 13. Whistleblowing

Whistleblowing

47. (1). (a) The Authority shall establish rules giving the authorization for and governing the whistleblowing system.

(b) These rules must preserve:

(i) the principles of fairness, lawfulness and purpose of the processing;

(ii) the principles related to the proportionality as the limitation of the scope, accuracy of the data which will be processed;

(iii) the principle of openness with delivering an adequate collective and individual information on:

- the scope and purpose of the whistleblowing;
- the processing of reporting;
- the consequences of the justified and unjustified reporting;
- the way of exercising the rights of access, to rectification, deletion as well as the competent authority to which a request can be made;
- the third party which may receive personal data concerning the informer and the person who is implicated in the scope of the processing of the reporting (for example the internal audit service if the "manager of the reporting" needs to verify some points).

The person who is implicated shall be informed as soon as possible by the "manager of the reporting" of the existence of the reporting and about the facts which he/he is accused for in order to exercise the rights set up in this model law.

The information of the person who is implicated may be postponed in exceptional circumstances (e.g.: risk of proof destruction).

(iv) the technical and organizational rules;

(v) rules concerning the rights of the data subject by making clear that the right of access doesn't allow to access to personal data linked to a third person without his/her express and written consent;

(vi) the rules of notification to the Authority;