Elements for principle of fairness.

36. The elements necessary to implement the principle of fairness include—

(a) granting the data subjects the highest degree of autonomy with respect to control over their personal data;

(b) enabling a data subject to communicate and exercise their rights;

(c) elimination of any discrimination against a data subject;

(d) guarding against the exploitation of the needs or vulnerabilities of a data subject; and

(e) incorporating human intervention to minimize biases that automated decision-making processes may create.

PART VI—NOTIFICATION OF PERSONAL DATA BREACHES

Categories of notifiable data breach.

37. (1) For the purpose of section 43 of the Act, a data breach is taken to result in real risk of harm to a data subject if that data breach relates to —

(a) the data subject's full name or identification number and any of the personal data or classes of personal data relating to the data subject set out in the Second Schedule; or

(b) the following personal data relating to a data subject's account with a data controller or data processor—

(i) the data subject's account identifier, such as an account name or number; and

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

(2) A breach of any personal data envisaged under sub-regulation (1) amounts to notifiable data breach under section 43 of the Act.

(3) The personal data or classes of personal data set out in the Second Schedule excludes —

(a) any personal data that is publicly available; or

(b) any personal data that is disclosed to the extent that is required or permitted under any written law.

(4) The personal data referred to in sub-paragraph (3) (a) shall not be publicly available solely because of any data breach.

Notification to Data Commissioner.

38. (1) A notification by data controller to the Data Commissioner of a notifiable data breach under section 43 of the Act shall include—

(a) the date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;

(b) a chronological account of the steps taken by the data

controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;

(c) details on how the notifiable data breach occurred, where applicable;

(d) the number of data subjects or other persons affected by the notifiable data breach;

(e) the personal data or classes of personal data affected by the notifiable data breach;

(f) the potential harm to the affected data subjects as a result of the notifiable data breach;

(g) information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissioner of the occurrence of the notifiable data breach to—

(i) eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or

(ii) address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

(h) the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach; or

(i) contact information of an authorized representative of the data controller or data processor.

(2) Where the data controller intends not to communicate a notifiable data breach to a data subject affected by such breach, under the conditions set out in section 43(1) (b) of the Act, the notification to the Data Commissioner under sub-regulation (1) shall additionally specify the grounds for not notifying the affected data subject.

PART VII—TRANSFER OF PERSONAL DATA OUTSIDE KENYA

Interpretation of the Part VII.

39. In this Part, unless the context otherwise requires —

(a) "data in transit" means personal data transferred through Kenya in the course of onward transportation to a country or territory outside Kenya, without the personal data being accessed or used by, or disclosed to, any entity while in Kenya, except for the purpose of such transportation;

(b) "recipient" means an entity that receives in a country or

territory outside Kenya the personal data transferred to the recipient by or on behalf of the transferring entity, but does not include an entity that receives the personal data solely as a network service provider or carrier;

(c) "transferring entity" means an entity that transfers personal data from Kenya to a country or a territory outside Kenya but does not include an entity dealing with data in transit; and

(d) "relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes.

General principles for transfers of personal data out of the country.

40. A data controller or data processor who is a transferring entity shall before transferring personal data out of Kenya ascertain that the transfer is based on—

(a) appropriate data protection safeguards;

(b) an adequacy decision made by the Data Commissioner;

(c) transfer as a necessity; or

(d) consent of the data subject.

Transfers on the basis of appropriate safeguards.

41. (1) A transfer of personal data to a another country or a relevant international organisation is based on the existence of appropriate safeguards where—

(a) a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations; or

(b) the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.

(2) Where a transfer of data takes place in reliance on sub-regulation (1)—

(a) the transfer shall be documented;

(b) the documentation shall be provided to the Commissioner on request; and

(c) the documentation shall include—

(i) the date and time of the transfer;

(ii) the name of the recipient;

(iii) the justification for the transfer; and

(iv) a description of the personal data transferred.

Deeming of appropriate safeguards.

42. For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49 (1) of the Act and these Regulations, any country or a territory is taken to have such

safeguards if that country or territory has—

(a) ratified the African Union Convention on Cyber Security and Personal Data Protection;

(b) a reciprocal data protection agreement with Kenya; or

(c) a contractual binding corporate rules among a concerned group of undertakings or enterprises.

Binding corporate rules.

43. (1) The contractual binding corporate rules contemplated under regulation 41 shall be valid if they—

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in sub-regulation (2).

(2) The binding corporate rules referred to in sub-regulation (1) shall specify—

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of another country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles;

(e) the rights of data subjects in regard to processing and the means to exercise those rights;

(f) the complaint procedures; and

(g) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules.

Transfers on the basis of an adequacy decision.

44. (1) A transfer of personal data to another country or a relevant international organization is based on an adequacy decision where the Data Commissioner makes a decision that—

(a) the other country or a territory or one or more specified sectors within that other country, or

(b) the international organization, ensures an adequate level of protection of personal data.

(2) The Data Commissioner may publish on its website a list of the countries, territories and specified sectors within that other country

and relevant international organisation for which the Data Commissioner has made a decision that an adequate level of protection is ensured.

Transfers on the basis of necessity.

45. (1) Personal data may be transferred to another country or territory on the basis of necessity is such a transfer is necessary for any of the purpose outlined under section 48 (c) of the Act.

(2) Prior to making a transfer under sub-regulation (1), a transferring entity shall ascertain that—

(a) that the transfer is strictly necessary in a specific case outlined under section 48(c) of the Act;

(b) there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.

(3) This section does not affect the operation of any international agreement in force between Kenya and other countries in the field of judicial co-operation in criminal matters and police co-operation.

Transfer on basis of consent.

46. (1) In accordance with section 25 (g) of the Act, in the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity, a transfer or a set of transfers of personal data to another country shall take place only on the condition that the data subject—

(a) has explicitly consented to the proposed transfer; and

(b) has been informed of the possible risks of such transfers.

(2) Without limiting the generality of sub-regulation (1), a data controller or processor must seek consent from a data subject for the transfer of sensitive personal data, in accordance with section 49 of the Act.

Subsequent transfers.

47. (1) Where personal data is transferred in accordance with this Part, the entity effecting the transfer shall make it a condition of the transfer, that the data is not to be further transferred to another country or territory without the authorisation of the transferring entity or another competent authority.

(2) A competent authority may give an authorisation under sub-regulation (1) only where the further transfer is necessary for a law enforcement purpose.

Provisions for the agreement to cross boarder transfer.

48. A transferring entity may enter into a written agreement with the recipient of personal data, which shall contain provisions relating to—

(a) unlimited access by the transferring entity to ascertain the existence of a robust information system of the recipient for storing the personal data; and

(b) the countries and territories to which the personal data may be transferred under the contract.