African Union, Southern African Development Community and South Africa Legislation review*: A review of data subject's rights with regards to automated decision making systems, the right to consent, the right to be informed and the right to object as in the Data Protection Framing in the African Union's Convention on Cyber Security and Personal Data Protection, Southern African Development Community Model Law on Data Protection and South Africa's Protection of Personal Information Act.

Prepared by Rumbidzai Matamba and Chenai Chair
The review was done in the period of February 2020 to October 2020 and the comments are the opinions of the authors

Year	Title	Framing	Comments
2014	**African Union Convention on Cyber Security and Personal Data Protection (Signed by 14 countries Ratified by 8 countries as of 18 June 2020)** ***South africa is not a signatory**	The convention sets forth the security rules essential for establishing a credible digital space for electronic transactions, personal data protection and combating cybercrime. **Article 8: Objectives with respect to personal data** Instructs State Parties to establish legal frameworks aimed at strengthening fundamental rights and public freedoms **Article 10: preliminary personal data processing formalities** Personal data processing shall be subject to a declaration before the National Protection Authority which each country must appoint. **Article 12:** the national protection authorities shall ensure that Information and Communication Technologies do not constitute a threat to public freedoms and the private life of citizens. **Article 13: Basic principles governing the processing of personal data** Principle of consent and legitimacy of personal data processing - Processing of personal data shall be deemed to be legitimate where the data subject has given his/her consent. The requirement of consent may however be waived where the processing is necessary for compliance with a legal obligation to which the controller is subject; performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; performance of a contract to which the data subject is party; or in order to take steps at the request of the data subject prior to entering into a contract; or to protect the vital interests or fundamental rights and freedoms of the data subject.	The definition of 'consent of data subject' in the Convention requires the manifestation of "…informed will". What is this measured against? How do you regulate whether one is informed electronically? People know to click 'yes' or 'next' or the highlighted button to proceed when using electronic resources, how do we regulate whether they are informed enough to consent? The type of language used in policy statements or terms of service contains a lot of legalese in most cases and there is rarely the option to translate the terms and conditions of service into a local language. **Article 8** which relates to personal data tasks each country with establishing legal frameworks to strengthen fundamental rights and public freedoms. This necessitates the need for the enactment of specific legislation, by every State Party, regulating data rights.

		Principle of lawfulness and fairness of personal data processing - The collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently. Principle of transparency of personal data processing - The principle of transparency requires mandatory disclosure of information on personal data by the data controller Principle of confidentiality and security of personal data processing - Personal data shall be processed confidentially and protected, in particular where the processing involves transmission of the data over a network. Where processing is undertaken on behalf of a controller, the latter shall choose a processor providing sufficient guarantees. It is incumbent on the controller and processor to ensure compliance with the security measures defined in the Convention. **Article 14: specific principles for the processing of sensitive data** State parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation. Political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject. **Article 15: interconnection of personal data files** The interconnection of files laid down in Article 10.4 of the Convention should help to achieve the legal or statutory objectives which are of legitimate interest to data controllers. This should not lead to discrimination or limit data subjects' rights, freedoms and guarantees, should be subject to appropriate security measures, and also take into account the principle of relevance of the data which are to be interconnected. **Article 16: right to information** The data controller shall provide the natural person whose data are to be processed with the following information: his/her identity and of his/her representative, if any; the purposes of the processing for which the data are intended; categories of data involved; recipient(s) to which the data might be disclosed; the capacity to request to be removed from the file; existence of the right of access to and the right to rectify the data concerning him/her; period for which data are stored; and proposed transfers of data to third countries. **Article 17: right of access** Any natural person whose personal data are to be processed may request from the controller, in the form of questions, the following: such information as would enable him/her to evaluate and object to the processing; confirmation as to whether or not data relating to him/her are being processed; communication to him/her of the personal data undergoing processing and any available	The prohibitions set in **Article 14** shall not apply to a few listed categories including where processing relates to data which are manifestly made public by the data subject and the processing of genetic data required for the establishment, exercise or defence of legal claims or when a judicial procedure or criminal investigation has been instituted. The question is what are you consenting to when you make certain sensitive data public? Especially because one cannot consent to the violation of inalienable rights such as human dignity. Further, section 35 rights (fair trial rights) are also inalienable so data cannot be processed without one's consent as that would be illegal in South Africa (The South African Constitution, 1996). The Convention does not list the procedure to be followed when one wants to exercise their right to object to their data being processed (**Article 18**). This is left to the judiciary which can find guidance from the landmark Spanish case between Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos (AEP) Mario Costeja Gonzalez (case no C-131/12, 13-5-2014)

		information as to their source; information as to the purpose of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the data are disclosed. **Article 18: right to object** Any natural person has the right to object, on legitimate grounds, to the processing of the data relating to him/her. He/she shall have the right to be informed before personal data relating to him/her are disclosed for the first time to third parties or used on their behalf for the purposes of marketing, and to be expressly offered the right to object, free of charge, to such disclosures or uses. **Article 19: right of rectification or erasure** Any natural person may demand that the data controller rectify, complete, update, block or erase, as the case may be, the personal data concerning him/her where such data are inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage are prohibited **Article 25: legal measures** Rights of citizens – in adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others. **Article 29: offences specific to Information and Communication Technologies** Content related offences – criminal offences limited to child pornography, pornography, racist, and xenophobic materials.	Article 19 provides for the right to rectification or erasure of personal data. How often does this happen? What are the processes that one must take to exercise this right? It's a strenuous process to get google to delete information about you off the internet. (Look up those facebook cases where the court discusses the complications involved in asking a data controller or another individual to take down information that infringes on your rights) Article 29 which criminalizes offences specific to ICTs does not mention of LGBTQI+ hate crime
2013	**Southern African Development Community (SADC) Model Law on Data Protection**	Data protection recognised as fundamental to the development of the individual in a democratic society and the construction of well-being A principle of accountability is required of the data controller and his/her data processor according to the sensitivity of the processed data. Data is categorised according to its sensitivity; sensitive data and data that is not sensitive First mention of the right to consent/object: provision to the individual control of his/her own data via a right of access from which will result, among others, a right of rectification and opposition "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"	Project to develop a model law for the harmonization of telecommunications/ICT policies and regulations began in December 2008 Language is exclusionary i.e. 'his/her' and not 'their' which is gender neutral Consent requires an informed expression of will but there is no benchmark that this is measured against. What constitutes informed expression of will? **Part V** allows for the processing of what is classified as non-sensitive data without the consent of the data subject. The problem is that what is classified as non-sensitive data is subjective and there have been instances where what has been categorized as non-sensitive

		"Sensitive data: refers to certain personal data including 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, affiliations, trade-union memberships, gender and data concerning health or sex life. Refers also to any personal data 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." **Part V: General Rules on the Processing of Personal Data** The processing of non-sensitive data is permitted without the consent of the data subject, if necessary. The model law goes on to list the instances which necessitate this processing including when the data may be material as evidence in proving an offence. **Article 15:** The processing of sensitive personal data is prohibited unless the data subject has given his/her consent in writing for such processing unless the law or the National Protection Authority states that the prohibition cannot be lifted by the written consent of the data subject. The consent of the data subject can be withdrawn by the data subject at any time and without any explanation and free of charge. The Authority may determine the cases in which the prohibition to process the sensitive data cannot be lifted even with the data subject's consent. **Article 15 (4)** (a) (i) 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, **Article 16** 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 except where the law provides that the prohibition cannot be lifted even with the written consent of the data subject. The consent referred to above can be withdrawn by the data subject at any time without any motivation and free of charge. 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.	data was hacked and the privacy of whistle-blowers was at risk (J Lautier article) The South African Constitution (section 35) protects one against self-incrimination so data cannot be automatically processed without consent if it is to be used as evidence in proving an offence. Violation of one's section 35 rights (fair trial rights) and conflict with South African law so provision would not apply in South Africa. The Constitution offers more protection of data rights than the Model Law at this juncture. **Article 15** on the processing of sensitive data acknowledges that some rights are inalienable despite consent being given. **Subsection 4 of Article 15** literally states that if you are of a sexual orientation that is not considered conventional, basically all non-hetero persons, your data can be processed without your consent because their sexuality is considered an offence!

		Article 18 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 for necessitated by the litigation; 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 is necessary for scientific research and the Authority establishes the conditions of such processing. **Article 22** Where 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 set out below when recording the personal data or considering communication to a third party, and at the very latest when the data is first disclosed, unless it is established that the data subject is in receipt of 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 supporting information, as necessary to ensure fair processing 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.	

		Article 29 The Authority shall keep a register of all automatic processing operations of personal data. **Article 31** 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. **Article 32: Right of rectification, deletion and temporary limitation of access** 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 concerned is not complete or inaccurate. (b) Any person also has the right to obtain free of charge the deletion of, or prohibition of the use of, all personal data relating to him/her that is incomplete or irrelevant 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 retention period. (2) The data subject has the right to obtain from the controller notification of all third parties to whom their personal data has been disclosed as well as rectification, deletion or temporary limitation pursuant to paragraph (1) unless this proves impossible or involves a disproportionate effort. **Article 33: Right of objection** 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 such data;	

		or (b) to be informed before personal data is 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. **Article 36: Decision taken purely on the basis of automatic data processing** 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. This prohibition 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 person must be given at least the chance to defend his/her point of view.	
2013	**Protection of Personal Information Act 4 of 2013**	''consent'' means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information **Section 5 – Rights of Data Subjects** A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3. This includes the right to be notified that personal information about him, her or it is being collected; his, her or its personal information has been accessed or acquired by an unauthorised person; to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information; to request, where necessary, the correction, destruction or deletion of his, her or its personal information; to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information; not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications; not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person; to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information; and to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information. **Section 11: Consent, justification and objection** Personal information may only be processed if the data subject or a competent person where the data subject is a child consents to the processing.	The Act has come into force incrementally, starting with the sections giving effect to the office of the Information Regulator (section 1, Part A of Chapter 5, section 112 and section 113) in 2014. The remaining sections of the Act were supposed to come into force in 2019. As at 22 June 2020, the President announced the commencement of the following sections from the first of July 2020: sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3); and, from the 30th of June 2021, the commencement of sections 110 and 114(4). The President of South Africa has proclaimed the POPIA commencement date to be 1 July 2020

		A data subject may object, at any time, to the processing of personal information. If a data subject has objected to the processing of personal information the responsible party may no longer process the personal information. **Section 12: Collection directly from the data subject** Personal information must be collected directly from the data subject. It is not necessary to comply with this provision if the information is contained in or derived from a public record or has deliberately been made public by the data subject; the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source; collection of the information from another source would not prejudice a legitimate interest of the data subject; collection of the information from another source is necessary– to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997); for the conduct of proceedings in any court or tribunal that have 10 commenced or are reasonably contemplated; in the interests of national security; or to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied; compliance would prejudice a lawful purpose of the collection; or compliance is not reasonably practicable in the circumstances of the particular case. **Section 13: Collection for specific purpose** Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Steps must be taken in accordance with section 18(1) to ensure that the data subject is aware of the purpose of the collection. **Section 18: Notification to data subject when collecting personal information** If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of the information being collected and where the information is not collected from the data subject, the source from which it is collected. It is not necessary for a responsible party to comply with this provision if the data subject or a competent person where the data subject is a child has provided consent for the non-compliance	

		Section 22: Notification of security compromises Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator; and the data subject, unless the identity of such data subject cannot be established. **Section 23: Access to personal information** A data subject, having provided adequate proof of identity, has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject and request from a responsible party the record or a description of the personal information about the data subject held by the responsible party. **Section 24: Correction of personal information** A data subject may, in the prescribed manner, request a responsible party to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of section 14. **Section 26: Prohibition on processing of special personal information** A responsible party may, subject to section 27, not process personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. **Section 69: Direct marketing by means of unsolicited electronic communications** The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject has given his, her or its consent to the processing. **Section 71: Automated decision making** Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.	