VERBATIM

December 2024

ISSUE 110

PROTECTION OF PERSONAL INFORMATION ACT, 2017 (POPIA) – DRAFT REGULATIONS RELATING TO THE PROCESSING OF DATA SUBJECT'S HEALTH OR SEX LIFE BY CERTAIN RESPONSIBLE PARTIES

Recently, the Information Regulator circulated draft Regulations on Processing Health and Sex Life Data under the Protection of Personal Information Act ('POPIA'). The draft Regulations emphasise heightened protection for sensitive personal information, particularly concerning health and sexual matters. By introducing:

- specific consent requirements,
- a structured assessment process for legitimate interests, and
- mandatory regulatory oversight,

these regulations aim to enhance accountability among responsible parties. In contrast, existing privacy laws often provide broader frameworks without such detailed stipulations for sensitive data types.

Applicable to listed responsible parties processing personal information regarding data subjects' health or sex life for circumscribed activities, the proposed Regulations govern, *inter alia*, the provision of consent, cross-border transfers of information, retention of records, and destruction of information.

Health information is defined as personal information or an opinion relating to the physical and mental health of a data subject, including:

- the provision of healthcare services; and/or
- any testing, treatment, and diagnosis which reveals information about his/her health status, and
- the decision of such a person regarding any illness, disability, or injury.

Sex life information is defined as any information that may reveal a data subject's gender identity, sexual orientation, or sex.

It is intended that the draft regulations will apply to the following responsible parties:

- Insurance Companies;
- Medical Schemes;
- Medical Scheme Administrators;
- Managed Healthcare Organisations;
- Administrative Bodies;
- Pension Funds;
- Employers
- Operators of Administrative Bodies, Pension Funds and Employers.

Not all of the draft regulations will apply equally to all of the listed responsible parties. For example,

1. **Insurance companies, medical schemes, medical scheme administrators, and managed healthcare organisations** will have to obtain consent from the data subject or competent person or the next of kin of a data subject before processing the data subject's health or sex life information. In addition, where any of these responsible parties are required to process health or sex life information for purposes set out in section 32(i)(b) of POPIA*, they will have to obtain authorisation from the Information Regulator to do so.

*A reminder: Section 32(i)(b) of POPIA states:

(1) The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in section 26, does not apply to the processing by:
  (a) …
  (b) insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for:
    i. assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;
    ii. the performance of an insurance or medical scheme agreement; or
    iii. the enforcement of any contractual rights and obligations;

2. Administrative bodies, pension funds, employers and institutions that work for them may, without consent or authorisation, process health and sex life information if necessary for:

  a. the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
  b. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

The draft regulations that will apply to all the listed responsible parties, including pension funds, employers, administrative bodies and their service providers, include the following:

1. **Legitimate Interest Assessment (LIA)**
   Many rely on POPIA's "legitimate interest" provisions to process information without consent. Under the proposed regulations, responsible parties may be required to perform a Legitimate Interest Assessment ("LIA") to identify the legitimate interests and decide whether the identified legitimate interest is appropriate to use as a lawful basis for processing personal information.

   The proposed LIA is a three-part assessment:

   Part 1: **A Purpose Test** to identify the legitimate interest by setting out the purpose for processing health or sex life information concerning a data subject, as well as the benefits associated with the responsible party processing such information;

   Part 2: **A Necessity Test** to determine if the processing of such personal information is necessary to achieve the goal/purpose; and whether there are no less intrusive methods that can be used to achieve the goal/purposes; and

   Part 3**: A Balance Test** which requires a responsible party to balance their legitimate interest against the interests and rights of the data subject. They must conduct this test by determining the relationship between the responsible party and the data subject, as well as identify the type of personal information being processed and whether it falls within the ambit of special personal information as envisaged in section 26 of the Act.

2. **Appropriate Safeguards**
   The responsible party is responsible for maintaining the confidentiality and integrity of such information in its possession or under its control by taking appropriate, reasonable technical and organisational measures in accordance with section 19(1) of POPIA;

3. **Transfer of Health and Sex Life Information outside of the Republic**
   The responsible party may not transfer the health or sex life information of a data subject to a third party in a foreign country unless one or more of the conditions set out in section 72(1) of the Act are met.

4. **Retention of Records**
   The responsible parties must ensure that they keep records containing health or sex life information of data subjects in accordance with section 13 of the National Health Act 61 of 2003, the National Archives of South Africa Act 43 of 1996, the Promotion of Access to Information Act 2 of 2000 and in accordance with the relevant provisions of POPIA and any other relevant legislation. In the event that a policy, employment contract or other relevant agreement is rejected or terminated, a responsible party is mandated to destroy the data subject's health or sex life information as soon as practicably possible.

These draft regulations represent a significant step towards enhancing data protection measures related to sensitive personal information in South Africa, emphasising the need for responsible handling of health and sex life data by various organisations.