

Advice re planning of document retention and disposal to meet the requirements of the Protection of Personal Information Act, 2013 (POPIA)

Advice prepared by Dr Peter Tobin (drpetertobin@gmail.com). This should not be interpreted as legal advice but as operational advice as to how to address the requirements of the POPIA. NOTE: This advice should be used in conjunction with any relevant organisation policy, process or procedure or amended to fit such. Correct as at 5 July 2018.

1 Retention requirements in POPIA

1. There are no specific retention periods for records mentioned in POPIA. POPIA is a form of umbrella legislation which draws on the specific requirements of other applicable legislation within the context of the legislative universe for an entity operating in South Africa.
2. Retention of records is covered under Condition 3 Purpose Specification, Section 14 (sub-sections 1 to 4) under sub-heading Retention and Restriction of Records. For ease of reference the relevant text is included here:

Retention and restriction of records

14. (1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—
- (a) retention of the record is required or authorised by law; 30
 - (b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
 - (c) retention of the record is required by a contract between the parties thereto; or
 - (d) the data subject or a competent person where the data subject is a child has consented to the retention of the record. 35
- (2) Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.
- (3) A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must— 40
- (a) retain the record for such period as may be required or prescribed by law or a code of conduct; or
 - (b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, 45 taking all considerations relating to the use of the personal information into account, to request access to the record.
- (4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2). 50

2 Suggested approach to meet POPIA requirements Section 14 (1 to 4)

Step 1: Identification of retention requirements

1. Identify your organisation's legislative universe (that body of laws and regulations which determine the environment in which your organisation operates); this includes national (South Africa), regional (SADC), continental (African Union) and global (beyond Africa e.g. EU, USA and other relevant legislation such as GDPR or Sarbanes-Oxley Act)
2. Identify any industry mandatory codes or standards under which your organisation operates (e.g. IATA for airline industry)

3. Identify any voluntary codes or standards, models or frameworks to which your organisation subscribes
4. Identify any internal policies which influence record retention periods
5. Identify any contractual commitments to stakeholders (e.g. suppliers, employees, customers)
6. Compile these requirements into an integrated matrix showing retention periods per requirement

Step 2: Identification of records processed containing personal information as defined in POPIA

1. Develop a comprehensive view of your organisation structure which will allow you to engage with relevant stakeholders who may be record owners for personal information (PI) (refer to POPIA Chapter 1 for detailed definitions of PI)
2. Engage with stakeholders using the Personal Information Diagnostic (PID) Tool to identify PI under the record ownership of the responsible individual
3. Complete the PID for all relevant records

Step 3: Match requirements to records processed

1. For each record containing PI which is processed identify the applicable retention requirements from Step 1
2. Determine the longest retention requirement as the result of step 3.1
3. Assign the retention period to specific records and update the records to show the relevant retention period
4. Establish a records management retention system which has built-in automated reminders which will trigger notification of the end of the retention period

Step 4: Record document disposal at the end of the retention period

1. Create a record keeping system which will indicate the record disposal method used (select applicable from the following list):
 - a. Physical destruction (typically used with paper records) compliant with Section 14.1.5
 - b. Electronic destruction (typically a form of deletion or erasure used with digital records such as on servers, laptops, mobile devices etc) Section 14.1.5
 - c. Return of records to data subject and subsequent destruction (4.1.a) or deletion (4.1.b)
 - d. De-identification of records which are to be retained for statistical or historical purposes (in line with POPIA Section 14.1.4 – also see Chapter 1 definition of de-identify)