Virtucomp

POPI Audit Assessment Guidance

PHONE: +27 41 020 0215 FAX: +27 86 225 7057 MOBILE: +27 83 644 6962 WEB: www.virtucomp.co.za
ADDRESS: 1st Floor – Landbank Building, 51 Newton Street, Newton Park, 6001

Why undertake a data protection audit?

Information is a valuable asset and resource to any organisation. The POPPI Act ("the Act") sets out rules regarding the managing, handling and utilisation of a particular form of information, i.e. 'personal data'. These rules are the 'data protection principles'. Organisations may utilise personal data for many different reasons, for example staff administration, the provision of goods or services to customers, marketing strategies, prevention of money laundering etc. It is important to ensure that the utilisation of personal data accords with the requirements of the Act.

What is the benefit of undertaking a data protection audit?

A data protection audit operates as a control mechanism and may identify irregularities or system weaknesses regarding the organisation's handling of personal data – i.e. compliance with the data protection principles. These weaknesses may include a lack of security, which may lead to inappropriate use of the personal data, the collection of unnecessary or irrelevant personal data, or the over-long retention of personal data.

The audit may also reveal weaknesses in respect of compliance with the rights of individuals, such as the right of access, or the obligation to notify the Supervisor of the types of processing of personal data undertaken by the organisation.

The audit may lead to the identification of processes, procedures or measures that need to be implemented, supplemented or amended in such a way as to ensure compliance with the Act or gauge the level of awareness of data protection as part of the business function within the organisation.

The audit may also reveal opportunities for financial savings, for example, in the case of monitoring retention periods the audit may result in the organisation taking steps to implement more effective records management and free up office space or substantially reduce expensive archiving and/or offsite storage costs.

What areas does this assessment audit toolkit cover?

Many business areas should be included when undertaking a data protection audit, although it may prove difficult, and be resource-intensive, to undertake a full audit across the entire business function at the same time. This assessment toolkit is not a full data protection audit but identifies different areas to enable an incremental approach to auditing.

This allows the organisation to choose which area it feels appropriate to address first. As with many other audits, there may already be significant documentation in place that will enable the questions to be answered. However, depending upon the size and nature of the organisation, it may not be necessary to include responses to all questions.

The audit areas are set out separately in the following sections:

- Compliance and awareness – Audit Section 1
- Conditions for lawful processing of personal information – Audit Section 2
- Record retention – Audit Section 3
- Security of personal data – Audit Section 4
- Requests for personal data – Audit Section 5

- Unsolicited electronic communications – Audit Section 6

Each of these audit areas should be undertaken in respect of both client information and staff information.

DEFINITIONS AND PURPOSE

Legal Term	Legal Definition	Substitution word (if different)
data subject	the person to whom personal information relates	
electronic mail or e-mail	any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient	
filing system	any structured set of personal information which is accessible according to specific criteria	
information matching programme	the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about 10 or more data subjects with one or more documents that contain personal information of 10 or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject	
information protection officer	a— (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17 of the Promotion of Access to Information Act; or (b) private body means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act	
operator	a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct	

	authority of that party	
personal information	information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person; (d) the blood type or any other biometric information of the person; (e) the personal opinions, views or preferences of the person (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person	
processing	any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt,	

	recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as blocking, degradation, erasure or destruction of information	
public communications network	an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services	
public record	a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body	
record	any recorded information— (a) regardless of form or medium, including any of the following: (i) Writing on any material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under the control of a responsible party;	

	(c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence	
re-identify	in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that— (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject	
responsible party	a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information	
subscriber	any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services	

Audit Section 1- Compliance and awareness

This section is divided into the following parts:

- Compliance – corporate compliance and privacy awareness

This part seeks to identify the mandates for privacy protection and assesses the level of understanding and awareness at senior level.

- Staff training and awareness

This part seeks to assess the level of awareness of staff and identify what training is in place.

Audit Section 2 - Conditions for lawful processing of personal information

This section looks at compliance with the following data protection principles:

1. ACCOUNTABILITY

The responsible party must ensure that the principles set out in this Chapter and all the measures that give effect to the principles are complied with.

2. PROCESSING LIMITATION

- Personal information must be processed—
  (a) lawfully; and
  (b) in a reasonable manner that does not infringe the privacy of the data subject Personal information must be updated consistently, PI must be accurate and complete
- Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive
- Personal information may only be processed if—
  - the data subject consents to the processing
  - processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party
  - processing complies with an obligation imposed by law on the responsible party
  - processing protects a legitimate interest of the data subject
  - processing is necessary for the proper performance of a public law duty by a public body
  - processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied
- Individuals have the right to request confirmation of their data from a company, to enquire about their PI and to make corrections to that information

3. PURPOSE SPECIFICATION

- Data can only be collected for a specific, explicit and lawful purpose
- The processing of personal data must be compatible with the stated purpose of collection or must be legally complaint
- Personal information related to sensitive issues like race, health or politics have their own distinct rules under this Bill

4. FURTHER PROCESSING

- Personal information that will be processed further than the initial purpose of collection must comply with the conditions

5. INFORMATION QUALITY

The responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

6. TRANSBORDER INFORMATION FLOWS

Personal data shall not be transferred to a country or territory outside the country unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Each of these areas should be reviewed separately in respect of customers and staff.

Audit Section 3 - Record Retention

The Act does not specify how long personal data should be retained as the Act applies to many different organisations. The time for retention also depends on what type of information is held, the purpose for holding it and whether there are legal obligations requiring the retention of that particular information.

This applies to any personal data held, whether that is computerised or paper records, digital images, cctv or voice recordings. At the end of its lifetime, information must be destroyed securely and appropriately in accordance with the Act. It is therefore important that any organisation understands what information it holds and why, and therefore be able to identify any relevant legal or industry-standard retention periods.

A records' retention policy and a records' destruction policy targeted at the organisation's particular requirements and obligations should be developed, and regularly reviewed, to ensure compliance with this principle.

Audit Section 4 - Security of Personal Data

Access to information should be on a 'need to know' basis.

With this in mind, it is recommended that organisations:

- Conduct an audit identifying the types of information held, listing all information repositories and their location;
- Chart personal information flows both within the organisation and outside it, listing all third parties to which information may be disclosed and assess these disclosures to ensure they are legitimate;
- Examine access rights to information across the various identified repositories;
- Divide the organisation into functional units and assess whether access rights are appropriate based on the needs of each functional unit. There may be sub-divisions within each functional unit where access rights could be limited, or extended;
- Based on an analysis of information repositories and data flows, investigate with your IT team the possibility of installing filters, and creating tiered access to subsets of information;
- Review logging and reporting functionality for all systems holding information;

Examine other system controls, For example:

- Printer connections
- Copy facilities
- Necessity of enabled ports for USB or disks;

Conduct regular reviews of access control and user provisioning polices, especially with regard to situations where a user's role and duties within the organisation changes.

Audit Section 5 - Requests for Personal Data

One of these rights is the fundamental right of access to their information and the Act sets out the obligations in respect of this right.

Audit Section 6 - Unsolicited electronic communications

Many organisations rely on direct marketing for increased sales, diversification of products or services and generally increasing corporate awareness.

When direct marketing, in any format, is targeted at individuals, i.e. their personal data is used to send direct marketing, then that marketing is subject to the Act.

The rights of individuals are set out in Chapter 8 of the Act.

One of these rights, set out in Chapter 8, is the right to opt out from the use of their information for the purpose of direct marketing and individuals can exercise this right by writing to, or emailing, the organisation.