FACT SHEET

institutions and persons handling personal information under POPIA

The Protection of Personal Information Act, 2013 ("POPIA") imposes minimum standards on the way personal information is collected, received, stored, used, disclosed, and deleted.

Each business sector handles various kinds of personal and sensitive information. As an example, financial institutions handle confidential bank account information of data subjects and attorneys handle personal and confidential information relating to their clients.

Each business sector, trade or association is likely to already have obligations in handling personal information which are set out in: legislation, regulations, guidelines or rules from a regulator, industry codes, constitutions from associations, or in terms of the common law. It is imperative that institutions and persons comply with their specific rules as well as with the additional obligations imposed under POPIA.

This fact sheet sets out practical guidelines to assist institutions and persons to comply with their obligations under POPIA and should be read with the Guidance Note for POPIA Compliance attached to this fact sheet.

Collection of information

- Only collect Information that you need for a specific purpose (i.e. to service clients).
- Ensure that the client is aware of the purpose for which the information is collected and who the information will be shared with.

Destruction and deletion of information

- If you are no longer authorised to keep the personal information in your possession, ensure that it is disposed of securely.
- Physical records could be shredded, pulped, or burned.
- Electronic records could be deleted, meaning that a person without special technical IT skills would not be able to access or re-create the deleted records. If practical, electronic records should be destroyed by formatting the hard drive or using software to overwrite the records.

Storage of information

- Keep both physical and electronic information secure.
- Control access to physical files through access cards and locking files in a secure filing cabinet or vault.
- Ensure electronic information is secure with strong password protection, up to date antivirus software and firewalls and encrypted folders. USBs, mobile phones, and computer connections used to transfer information or store health records should be secure (for example, use encrypted USBs or allow access to records only through secure mobile applications). You must train staff in the proper handling of personal information held by you or by your organisation.

Sharing of information

- It is likely that all information relating to a client is confidential. You must have the informed consent of your client to disclose this information to another person. There are exceptions which are set out in the attached guideline.
- Ensure that contracts with third party service providers include POPI compliant clauses and appropriate indemnities regarding its safeguarding.

Retention of information

- Ensure that the information is relevant and up to date.
- Have a records policy that sets criteria for keeping information, or where appropriate, the specific
- retention periods for certain categories of information.

Requests for access to information

- Your clients have rights to see their personal information.
- You must allow a client to see their information on receipt of a valid request in the manner prescribed in your privacy policy if there are no lawful reasons to refuse access.
- Clients can require that their personal information be corrected or deleted.
- You may refuse to do so where the information is in your legitimate interest, but you must make a note of the challenge on the relevant record so that if questioned by the regulator you are able to appropriately respond.

itoo.co.za

@itooexpert
011 351 5000