IT GOVERNANCE NETWORK

The Eight Conditions for the Lawful Processing of Personal Information

Complying with the Protection of Personal Information Act

The Protection of Personal Information Act requires every public and private body to comply with the eight conditions that prescribe the minimum threshold requirements for lawful processing of personal information in South Africa. Public and private bodies should be mindful of the rights and remedies of persons to protect their personal information from processing that is not in accordance with the Protection of Personal Information Act.

Overview

These eight conditions set out the requirements for the lawful processing of personal information.

Accountability

The responsible party must ensure that the conditions for lawful processing of personal information set out in the Act, and all measures required to give effect, are complied with.

Processing limitation

Business processes provide the context for processing personal information – i.e. adequate, relevant, not excessive
Data collection must be proportionate to purpose – minimal
Data processing must be for a legitimate purpose (see PAIA)
Data subjects have given consent or necessary for a contract
Collection of personal data must be directly from the data subject unless it is contained / available in a public record
Limit the transfer of personal data to service providers
Data subject must be able to object, in the prescribed manner, at any time.

Purpose Specification

Collection of personal information must be for a specifically defined, lawful purpose related to a function or activity of the responsible party
Data subject must be aware of the purpose of collecting data
The purpose for processing personal information must be clear
Record retention must not be longer than necessary unless required by law, a contract or the data subject has consented
A record of the use of personal data to make a decision must be retained for such period required by a law or long enough for the data subject to request access to the record
As soon as practically possible destroy, delete or de-identify personal information
Destruction of personal information must be in a manner that prevents reconstruction in an intelligible form.

Further Processing Limitation

Further processing must be compatible with original purpose
Be aware of the potential consequences of further processing
Take note of any contractual rights and obligations
Take steps to prevent further processing of personal data
Data mining must not exceed original purpose of collection
Allow retention for historical, statistical or research purposes
Stop unlawful processing

Information Quality

Take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary
Be aware of the impact the integrity of personal data has on the purpose for collecting personal data
Note: master data must exclude unnecessary records
Note: master data must be secured, and accessed with the necessary granularity of control based on a need-to-know.

Openness

Only process personal data after updating PAIA manual, providing the Regulator with prior notification (if necessary), and informing the data subject.

The data subject must be aware of the collection of the data and the name and address of the responsible party, whether voluntary or mandatory, and of any law authorising collection, except if

- data subject is already aware
- all particulars are stated in PAIA information manual
- data subject consents to non-compliance
- information will be used without identifying data subject
- personal information is already in the public domain.

Data Subject Participation

Establish communication processes with data subjects (via the Information Officer)
Provide data subjects with access to personal information
Enable data subjects to request correction of personal data.

Security Safeguards

Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control and implement controls for maintaining integrity & confidentiality:

- Identify personal data (structured and unstructured) in all business processes (formal and informal)
- Identify business processing manual controls, application systems and IT process controls, including programmed procedures supporting the complete and accurate processing of personal data
- Maintain appropriate granularity in user access controls
- Maintain appropriate information resource protection
- Prevent data leakage (structured and unstructured data)
- Maintain the capability to detect security breaches
- Regularly review contractual obligations of third parties

Prohibit the processing of special personal information
Comply with Information Officer or Information Regulator.

Action Plan

Identify the legitimate business purposes for processing data
Establish a register of personal data being processed
Obtain prior authorisation from the Information Regulator of processing of personal data when required
Contact and communicate with data subjects
Obtain consent from data subjects when necessary
Enable data subjects to object to processing of personal data
Identify all reasonably foreseeable internal and external risks
Educate staff about the rights of individuals to be respected
Implement a system of internal control to maintain integrity
Secure structured and unstructured data
Reduce record retention, destroy unnecessary personal data
Change contracts and obligations of service providers (additional costs of outsourcing for increased security)
Appoint an Information Officer for data subjects to liaise with
Respond to requests of the Information Officer
Comply with requirements of the Regulator.

 www.itgovernance.co.za cell: 0825588732 info@itgovernance.co.za