IT GOVERNANCE NETWORK

Responsible Parties are to Act in a "Reasonable Manner"

The Protection of Personal Information Act places a significant burden on those deemed by the Act as "Responsible Parties" (control the purpose and means of processing information).

Responsible parties – those individuals who alone or in conjunction with others, determine the purpose of and means for processing personal information – are required by law to ensure that the conditions for the lawful processing of personal information, and all the measures that give effect to these conditions, are complied with.

Overview

Section 99 of the Protection of Personal Information Act allows a data subject or the Regulator to institute a civil action for damages in a court against a responsible party who is breach in any provision of the Act, whether or not there is intent or negligence on the part of the responsible party.

This places significant obligations on the business leaders identified as the "responsible parties" in control of the purpose and means for processing information. Business leaders who fail to fulfil their obligations defined in this Act can face civil claims for damages and be charged with a criminal offence.

It is the responsibility of the "Responsible Parties" identified by the CEO and listed in their organisation's PAIA manual to ensure that personal information under their control is processed lawfully and in a manner that does not infringe the constitutional rights of individuals to privacy.

What is the expected standard of Performance?

There are numerous provisions in the Protection of Personal Information Act that require the responsible party to act in a reasonable manner. The standard to determine whether a person acted reasonably is that of "objective foreseeability". In other words, would a reasonable person have foreseen the harm.

Any deviation from the standard of foreseeable harm establishes negligence, irrespective of whether the damage is due to the act of the responsible party or a service provider. Clearly, a responsible party can be held liable even though there is no apparent fault on his or her own. Of course contracting with a service provider or other processor of personal information on behalf of the responsible party, who does not meet or maintain the compliance requirements of the Protection of Personal Information Act would be negligent.

The burden of proof rests with the responsible party to demonstrate that he or she did properly and continuously assess the risk and take all the measures necessary to mitigate the risks to data subjects.

Lawful and Unlawful Processing

Every responsible party must ensure that the conditions set out in the Act regarding lawful processing of personal information and all the measures required, are implemented and continue to be effective.

The responsible party must ensure that the collection of personal information is for a specifically defined, lawful purpose related to a function of the responsible party's business processes. It is a requirement that the collection of personal information must be kept to a minimum. Consequently, collecting personal information beyond what is necessary for the purchased service or product can result in a claim for damages by a data subject as well as a possible charge for a criminal offence.

The responsible party is also required to have due regard for generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Obligations of Responsible Parties

Responsible parties are expected to be able to

- differentiate between personal and other data
- identify when prior notification to the Regulator is required before processing personal information
- identify and mitigate the risks to data subjects when collecting, processing and storing personal information
- establish communication with data subjects
- determine whether the conditions for lawful processing of personal information have been adhered to
- obtain permission to process personal information directly from the data subjects
- minimise the collection and processing of personal information
- determine whether the organisational and technical arrangements necessary for the protection of personal information are effective in protecting personal information
- search and retrieve personal information relating to a particular data subject's request
- supply the Regulator with answers to questions about the actions taken to ensure lawful processing and the protection of personal information
- take notice of and address compliance issues raised by the Information Officer
- establish suitable contracts with all "operators" (i.e. outsourced service providers, contractors and other third-parties)
- control the activities of "operators"
- prevent trans-border exchanges of personal information unless the conditions of the Act are adhered to
- secure unstructured data and prevent secondary use
- maintain appropriate granularity in user access controls
- immediately notify the Regulatory and data subjects of any breach in the processing of personal information
- respond to information and enforcement notices from the Regulator.

Consequences of not acting in a 'Reasonable Manner'

Settlement

The Regulator may, without investigating the complaint, use its best endeavours to secure a settlement between the parties and obtain assurance against repetition of the breach.

Civil Action

A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of the Protection of Personal Information Act, whether or not there is intent or negligence on the part of the responsible party.

Administrative Fine

The Regulator may request an 'infringer' to pay an administrative fine not exceeding R10 million.

Criminal Offences

Any person convicted of an offence in terms of this Act is liable to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment.