IT GOVERNANCE NETWORK

Impact of POPI on Contracts with Operators

Complying with the Protection of Personal Information Act

The Protection of Personal Information Act stipulates that every public and private body making use of operators (i.e. service providers and contractors) must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains generally accepted information security practices and procedures which may apply to it generally, or specifically.

Processing Personal Information

An operator processing personal information on behalf of a responsible party or another operator, must process such information only with the knowledge or authorisation of the responsible party. The operator must ensure that the personal information being processed on behalf of a responsible party is complete, accurate, not misleading and update to date.

The responsible party must clarify in its contracts with operators, the services that the operators are engaged to provide. The transfer of personal information to the operator must be limited to what is necessary for the operator to fulfil its contractual obligations.

Operators may not further process personal information unless the purpose is compatible with the original purpose for which it was collected unless consent was obtained.

Security Safeguards

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures.

Responsible parties are required to identify all reasonable foreseeable internal and external risks, and in terms of a written contract between the responsible party and the operator, ensure that the operator establishes and maintains the measures necessary to secure the confidentiality, integrity and accuracy of personal information in its possession or under its control.

Responsible parties may not enter into contracts with operators who cannot process personal information lawfully.

Technical and Organisational Measures

The contract between the responsible party and the operator must provide details of the technical and organisational measures that the responsible party has identified necessary for the operator to establish and maintain to address the internal and external risks to the processing of personal information, as identified by the responsible party.

The contract between the parties must also indicate that the responsible party understands the conditions under which the personal data will be handled by the operator.

The responsible party must verify that the operator has fulfilled its contractual obligations to implement and maintain effective technical and organisational measures to safeguard the data subjects' rights.

The responsible party must validate the effectiveness of the technical and organisational measures implemented.

Unauthorised Processing

Operators are required to detect unauthorised access to or acquisition of personal information and to notify the responsible party immediately it is detected.

An operator must be able to distinguish between processing that is in the legitimate interest of a responsible party, the operator and when it is unlawful. Operators must be able to identify who are their authorised personnel and maintain logs of the processing of personal information by authorised personnel. Adequate proof listings are required to substantiate the validity of the processing of personal information.

As operators are required to respond as soon as reasonably possible after the discovery of a compromise, they must have suitable processes and procedures in place to respond to any incidents and quickly restore the integrity of the systems.

Service Provider Capability

Data subjects have the right to expect that the operator adheres to the conditions for lawful processing of personal information and therefore operators must be transparent in all aspects of the processing of personal information.

Data subjects have the right to request the deletion and destruction of personal information when this information is not accurate, irrelevant, excessive, out of date, incomplete or obtained lawfully. Operators will be required to destroy all personal information obtained unlawfully and may be requested to provide assurance that this was done properly.

At least annually, the responsible party must verify that the operators' processing of personal information is lawful and the technical and organisational safeguards effective.

Suspension and Termination

When a contract between the responsible party and operator is suspended or terminated, and personal information remains in the possession of the operator, the operator becomes the responsible party.

Data subjects have the right to request the "operator" (who now is the responsible party) to confirm, free of charge, whether or not, as the responsible party, it holds personal information about the data subject.

At all times, operators must be able to identify and account for the personal information in their possession or under their control (and in the possession of sub-operators).

Operators (who are now the responsible parties) must enable data subject participation.