

MICROSOFT WHITE PAPER ON PERSONAL INFORMATION ACT, 2013 (POPIA)

The Protection of Personal Information Act, 2013 (POPIA) came into effect on 1 July 2020. The 12-month grace period for compliance commenced on 1 July 2020This means that private and public bodies, and anyone else who determines the purpose of, and means for, processing personal information (processing entities) now have until 30 June 2021 to comply with the Act's comprehensive requirements.

This White Paper sets out key provisions in POPIA but should not be read as an exhaustive summary of its provisions. Likewise, the controls detailed below should not be considered as representative of Microsoft's entire control framework. Furthermore, Microsoft's continuous development of its cloud service capabilities, combined with its focus on supporting and facilitating customers' compliance efforts, means that customers should consult their Microsoft representative for more information on available compliance technologies at the time of reading this White Paper.

Below we set out a high-level overview of the instances in which POPIA will apply to processing activities and the obligations which come with POPIA.



AM I SUBJECT TO POPIA?

POPIA APPLIES TO JURISTIC AND NATURAL PERSONS:

> Who are domiciled in South Africa; or Who are not domiciled in South Africa but use automated or non-automated means in South Africa, unless the personal information is only forwarded through South Africa.

YES

SO IF YOU PROCESS PERSONAL INFORMATION IN SOUTH AFRICA: POPIA will apply to you even if you are not domiciled in South Africa.



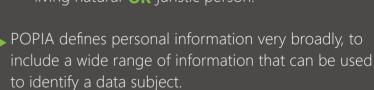
AM I PROCESSING PERSONAL INFORMATION?

"Processing" is defined broadly to include



WHAT IS PERSONAL **INFORMATION?**

PERSONAL INFORMATION IS: • Information relating to an identifiable, living natural **OR** juristic person.



Notably, POPIA refers to the personal information of juristic entities, meaning that businesses will be able to enforce their data protection rights under POPIA.



WHO CAN PROCESS PERSONAL INFORMATION?



A RESPONSIBLE PARTY

A responsible party is the person or entity that determines the purpose and means of processing personal information (i.e. determines the destiny of the information) and can act independently or jointly with other responsible parties.

> **RESPONSIBLE PARTY OBLIGATIONS UNDER POPIA**

Determining whether a person is a responsible party or an operator will not always be an easy exercise.

A person will have to assess its processing activities very closely.

The distinction is important, because it affects the rights and obligations that fall on responsible parties and operators respectively.



OPERATOR

An operator processes personal information for, or on behalf of, a responsible party in terms of a contract or mandate.

OPERATOR OBLIGATIONS UNDER POPIA



GENERAL PROCESSING PRINCIPLES

A RESPONSIBLE PARTY MUST COMPLY WITH ALL **8 CONDITIONS FOR LAWFUL PROCESSING, NAMELY:**

- **ACCOUNTABILITY:** You will be responsible for ensuring POPIA compliance
- **PROCESSING LIMITATION:** You must only process that information which you require
- **PURPOSE SPECIFICATION:** Personal information must be collected for a specific purpose

FURTHER PROCESSING

- LIMITATION: Further processing of personal information (i.e. outside original purpose) must be compatible with the original purpose of collection
- INFORMATION QUALITY: You must keep personal information
 - records accurate and up to date
- **OPENNESS:** You must disclose certain information to data subjects (i.e that their information is being collected, where it is collected from and how it is used
- SECURITY SAFEGUARDS: You must secure the integrity and confidentiality of personal information
- **ODE DATA SUBJECT PARTICIPATION:** You must allow data subjects to

access their personal information

OPERATOR

Responsible parties must conclude a written contract with operators to ensure that the operators establish and maintain measures that secure personal information.

the integrity and confidentiality of **INFORMATION**

CONTRACTS

OFFICER Responsible parties must appoint an Information Officer who is responsible

the provisions of POPIA.

for overseeing their compliance with **PRIVACY NOTICES**

Responsible parties must tell individuals

how their personal information is collected, why it is collected and how it will be used.

TRANS-BORDER INFORMATION

FLOWS

POPIA sets out restrictions on when personal information can be transferred outside South Africa.

O DATA SECURITY **AND BREACH**

NOTIFICATION

If there is a data breach, the responsible party may have to inform the affected individuals and the Information Regulator.

PROCESSING JUSTIFICATION

A responsible party must make sure processing in these circumstances:

- With consent • For performance of a contract
- In compliance with a legal obligation Legitimate interests
- Public law duty.

RECORD RETENTION

POPIA restricts the instances in which personal information can be retained by a responsible party.

OPERATOR CONTRACTS Operators must comply with the provisions of

the contract concluded with a responsible party.

DATA BREACH

Operators must notify the responsible party immediately of any suspected or actual data breach.



You manage your employee data on your IT systems

You are appointed to provide

payroll services to your client

your patient to a medical insurer

You provide information about

You send marketing emails to your client's customer list

You are likely a **Responsible Party**

You are Likely an

You are likely a

Operator

Responsible Party

You are likely an

Operator



CONTACT PERSONS

Andrea Campbell

E-MAIL: andrea.campbell@microsoft.com CALL: 27 (11) 361 7804

E-MAIL: asif.valley@microsoft.com

Colin Erasmus

Asif Valley

CALL: 27 (11) 361 8057

E-MAIL: colera@microsoft.com CALL: 27 (11) 361 7185