



# DECODING: SOUTH AFRICA'S PROTECTION OF PERSONAL INFORMATION ACT

An Exclusive Cheat-Sheet  
Curated By:



## I. POPIA OVERVIEW:

A comprehensive data protection law enacted by the Parliament of the Republic of South Africa aiming to protect personal information processed by public and private bodies of individuals within South Africa.

## II. KEY PARTIES UNDER POPIA:

### Data Subject:

The data subject is the person the information is about.

### Responsible Party:

The Responsible Party is the party that determines the purpose and means of processing Personal Information.

### The Operator:

The Operator is any party processing the Personal Information on behalf of the Responsible Party.

## III. RIGHTS OF DATA SUBJECTS: (SECTION 51)

- Right to be Notified
- Right to Access
- Right to Correction
- Right to Erasure
- Right to Object to Processing
- Right not to be subject to Automated Decision-Making
- Right to Redressal

## IV. KEY PRINCIPLES UNDER POPIA: (SECTION 4)

### ACCOUNTABILITY

Responsible parties are accountable for complying with POPIA.

### PROCESSING LIMITATION

Responsible parties can only process personal information for a justifiable reason.

### PURPOSE SPECIFICATION

Data subjects must know the purpose of processing their personal information.

### PROCESSING LIMITATION

Further processing of personal information must be compatible with the original purpose, or fresh consent must be obtained.

### ACCOUNTABILITY

Responsible parties are accountable for complying with POPIA.

### PROCESSING LIMITATION

Responsible parties can only process personal information for a justifiable reason.

## V. OBLIGATIONS UNDER POPIA

### TRANSPARENCY & PRIVACY NOTICE

Provide clear and accessible privacy notice to data subjects informing how personal information is collected, used, and processed. (Section 18)

### BREACH NOTIFICATION MECHANISMS

Implement procedures to detect, assess, and promptly report data breaches to the Information Regulator and affected data subjects. (Section 22)

### DATA SUBJECT REQUESTS

Establish processes for handling data subject requests. (Section 23 & Section 24)

### ROPA COMPLIANCE

Maintain the documentation of all processing operations (Section 17)

### SECURITY MEASURES

Implement appropriate technical and organizational measures to protect personal information. (Section 19)

### INFORMATION OFFICER (IO)

Ensure compliance, conduct Data Protection Impact Assessment, handle Data Subject Requests, undertake trainings etc. (Section 55)

## VI. ADDITIONAL OBLIGATIONS FOR DATA BREACH: (SECTION 22)

### Assess the Breach:

Determine the scope of the breach and data compromised and evaluate risks and potential harms.

### Contain the Breach:

Implement immediate actions to prevent the escalation of data breach after its discovery.

### Restore Data Security:

Take necessary steps for the restoration of Data Security

### Notify the Information Regulator:

Take necessary steps to notify the Information Regulator as soon as reasonably possible after the discovery of the data breach.

### Notify affected individuals:

Take necessary steps to notify the affected data subjects as soon as reasonably possible after the discovery of the data breach.

(Note: Methods of notification can be email, postal mail, website notice, public announcement.)

## VII. PENALTIES & OTHER ENFORCEMENT MEASURES



### ADMINISTRATIVE FINES SECTION 109

The Information Regulator can issue administrative fines up to **ZAR10 million (EUR 500,000 or \$520,000)** for certain contraventions of the Act.

### CRIMINAL PENALTIES SECTION 107

Parties found guilty of certain offences may be liable for **finances or imprisonment for a period up to 10 years**, or both.

### CIVIL REMEDIES SECTION 99

Data subjects can seek compensation for damage suffered due to a contravention of POPIA. This includes damages for both pecuniary and non-pecuniary loss.

### ENFORCEMENT NOTICE SECTION 95

The Information Regulator can issue an enforcement notice to enforce the provisions of POPIA.

