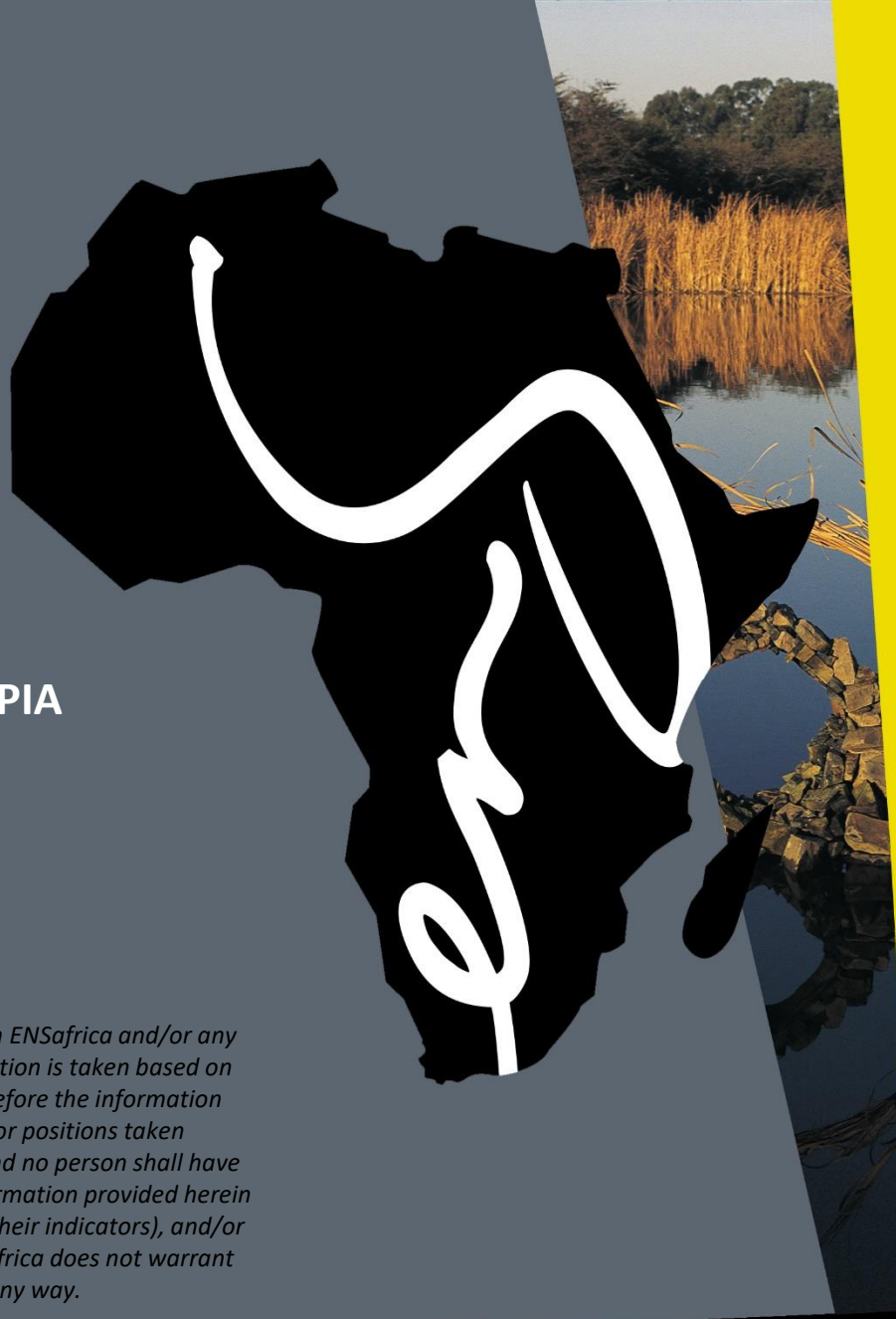

ENSafrica

Navigating data breaches in the age of POPIA

Ridwaan Boda

- Executive | Technology, Media and Telecommunications

Nicole Gabryk

- Executive | Dispute Resolution

Defending the Breach – security compromises POPIA

- Section 22 of POPIA imposes a mandatory security compromise notification obligation:

  *"Where there are reasonable grounds to believe that the **personal information** of a data subject has been **accessed or acquired** by **any unauthorised person,** the responsible party **must notify…**"*

- Regulator & Data Subjects
- Comprehensive Notification
- Quick Turnaround

Security Compromises – important concepts

Definition of Security Compromise?

- Not defined in POPIA : “personal data breach”, under the GDPR means “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data [information] transmitted, stored or otherwise processed”

Role Players: Operator or Responsible Party

- The responsible party, in terms of POPIA, bears the onus and obligation to make a report to the Regulator and affected data subjects. Ultimately, it is the responsible party who will be liable to affected data subjects for civil claims for damages, and/or to the Regulator for enforcement action, in the event that it fails to, *inter alia*, comply with its notification obligations

Do document the processes and findings of the response team. These are useful in strengthening cyber security, in addressing regulatory and legal requirements, as well as managing the concerns of staff and customers

Do take steps to prevent future attacks and consider using cyber-security specialists

Do consider obtaining appropriate insurance cover to mitigate losses to your organisation following a cyber-event

TOP TIPS

Don’t only react to cyber events - plan for them in a comprehensive incident response plan to avoid panic, ensure effective crisis management and mitigate losses

Don’t become so preoccupied with the breach that you overlook the legal consequences, including mandatory breach notifications, and consider seeking help from specialist data-protection attorneys.

Incident Response Planning 101

- The content of an incident response plan is not mandated, but it should be tailored to meet the needs of and resources available to each organisation

- Key aspects to be included in an incident response plan include:

  - the names and identities of the relevant members of the incident response team;
  - an evaluation of the risks posed to the business;
  - containment measures for any incident;
  - the process for conducting an initial assessment of any incident;
  - the remediation steps that should be implemented; and
  - a clear understanding of notification obligations