



Actuarial Society of South Africa

POPIA Training

7 May 2021

Important Legal Notice: The information in this document is provided for general information only. It is not legal or other professional advice. While we have taken reasonable steps to ensure it is accurate, Webber Wentzel accepts no liability or responsibility, to the extent allowed by law, if any information is, for any reason, incorrect or corrupted; or for any loss or damage that may arise from reliance on information in this document.

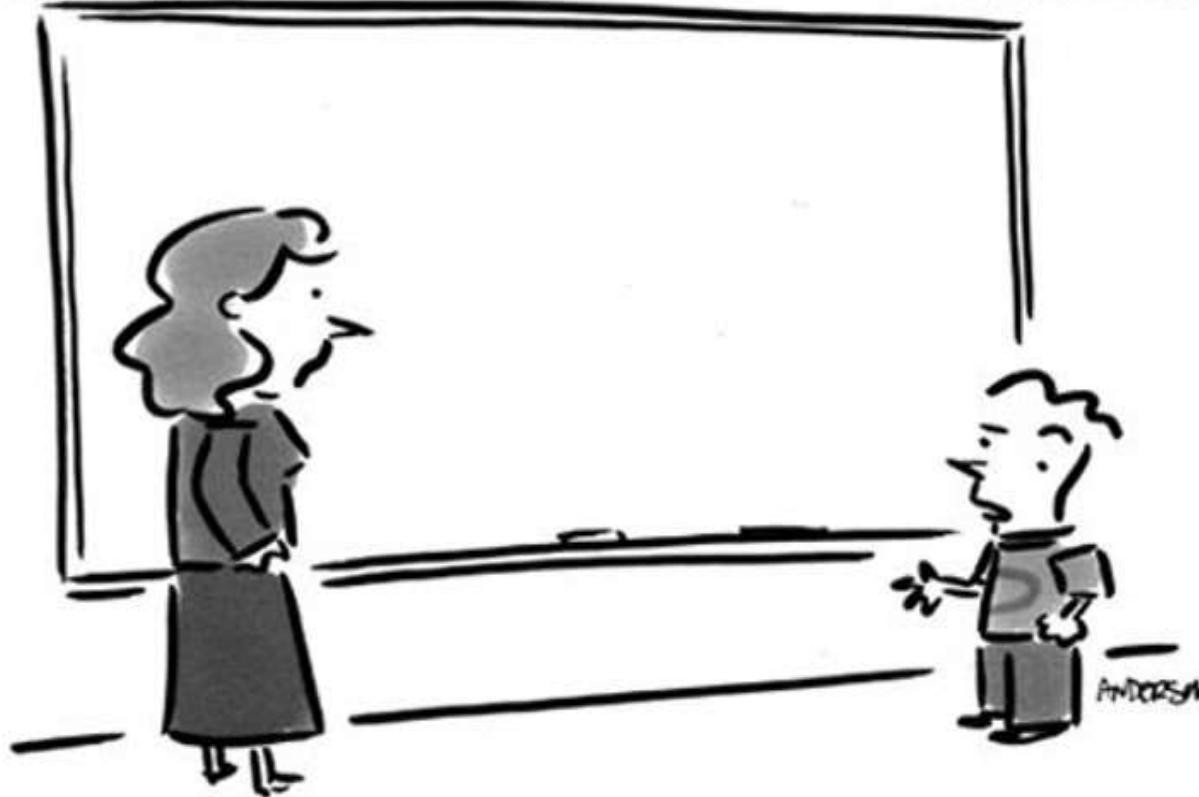
WEBBER WENTZEL

in alliance with > **Linklaters**

Protection of Personal Information Act (POPIA)

© MARK ANDERSON

WWW.ANDERSTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."



Roadmap

1. The POPIA timeline
2. Trends in the Insurance sector
3. POPIA definitions and what they mean for us?
4. The role players
5. Your processing practices
6. Overview of POPIA application
7. Eight conditions for lawful processing
8. Processing special information
9. Information officers
10. Automated Decision Making
11. Transborder data flows
12. Prior Authorisation
13. Security Breaches
14. The GDPR
15. Q&A



The POPIA timeline

The POPIA timeline

Days left to become POPIA compliant: 55



On 11 April 2014, certain sections of POPIA came into force:

- Section 1: Definitions
- Part A of Chapter 5: Regulating, amongst other things, the establishment, duties and powers of the Information Regulator
- Sections 112 and 113: Provisions regulating the right of the Minister of Justice and Constitutional Development to issue regulations, and the procedures that the Minister must follow in doing so.

Adv. Pansy Tlakula was appointed as Chairperson of the Information Regulator in October 2016

POPIA Regulations were published in December 2018 and President Ramaphosa declared that the majority of POPIA's provisions commenced on 1 July 2020, meaning that the one-year grace period will expire on **30 June 2021.**



Trends in the Insurance Sector



- **FROM** : Business being complicated



TO

- Business being complex

Resulting changes: Digitization

- New business - Being able to quote for new business online has become the norm. There's tremendous pressure to keep pace with customer expectations or lose prospective clients.
- Robotic automation process (RPA) - integrate artificial intelligence software and harvest – and use – the data they have.
- Pay-as-you-go insurance services, including new, innovative risk management products that provide niche cover for things such as cyber threats.



POPIA definitions and what they mean for us?

‘Personal information’

Information relating to an identifiable, living natural person, and where applicable juristic person, **including**:

- Race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth
- Education or the medical, criminal, employment or financial history of a person
- Identifying number, email address, telephone and physical address
- Online identifier
- Biometric information
- Personal opinions, views or preferences of the data subject
- Explicitly or implicitly private or confidential correspondence
- Views of others about that person
- Name if name would reveal information

‘Special personal information’

Separately defined and separately regulated.

The definition covers a data subject’s:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political persuasion
- Health
- Sexual life
- Biometric information
- Criminal behaviour

Implications – the scope of ‘personal information’

- Because it covers natural and juristic persons, POPIA regulates information of individuals, associations, bodies, companies, groups ...
- Definition of personal information is extremely broad
- Affects many people and many things we do with information
- All information about customers, employees, suppliers, other companies, investors, shareholders, affiliates
- **Beware:** Seldom do you receive personal information about people without also receiving special personal information
- In processing personal information, we are almost always processing special information
- E.g., Medical information and information on trade union membership of staff are both regulated distinctly as special personal information.

Past Ongoing obligation Future

POPIA **does not distinguish between past, present and future information processing.** This means that **records made in the past, present and future are regulated by POPIA.**

Processing



Any operation, or activity, or set of operations (whether or not by automatic means) concerning personal information, **including**:

- Collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; or
- Merging, linking, as well as restriction, erasure or destruction.

‘Record’ and ‘Consent’



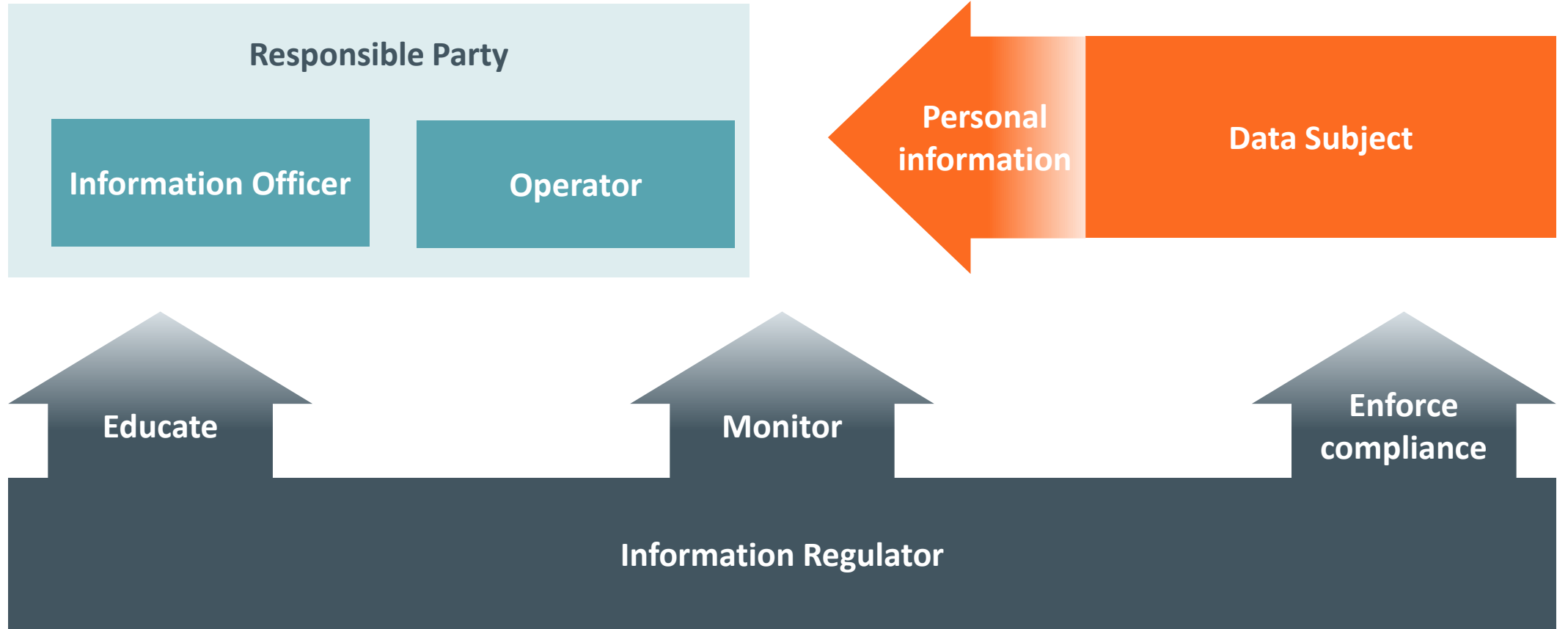
‘Record’ – any recorded information: Regardless of form or medium, including any of the following:

- Writing on any material;
- Information produced, recorded or stored with a tape-recorder, computer equipment or other device, and any material derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which visual images are embodied so as to be capable of being reproduced;
- In possession or under control of a responsible party;
- Whether or not it was created by a responsible party; and
- Regardless of when it came into existence.

‘Consent’ – voluntary, specific and informed expression of will in terms of which a person agrees to the processing of personal information.

(Special Personal Information may only be processed subject to the data subject’s explicit consent)

The role players





Insurance Actuaries' Processing Practices

WHAT ARE YOUR PROCESSING PRACTICES?

Where do you store personal information?

☐ Personal laptops?

☐ Central server?

☐ What personal information security controls do you use?

☐ Who do you share data subject personal information with?
Across departments?

☐ How often do you actively check the accuracy of personal information on record?

☐ How often is personal information that is no longer being used deleted?

☐ How will you handle a data breach?

☐ What is the internal data breach management process?



Application of POPIA

Co-responsibility

- Personal information includes so much, that compliance cannot be achieved by one party only - All parties need to take responsibility for POPIA.
- Anyone can 'sink the ship'!



Application of POPIA:

Lawful processing

- POPIA guides processing of personal information through eight conditions of lawful processing.
- The conditions are not applicable to some processing and some personal information.
- POPIA distinguishes special personal information, which is prohibited, unless provisions are applicable.
- Processing of personal information of children is prohibited under POPIA, unless provisions are applicable.
- POPIA sets out conditions for lawful processing of personal information for direct marketing purposes.
- Provides for codes of conduct to be complied with in sectors.

Rights of the data subject

- To be notified of processing of personal information
- To access of personal information
- To request correction, destruction or deletion
- To object to processing
- To not have info processed for direct marketing
- Not to be subject to a decision based on automated processing
- To submit a complaint
- To institute civil proceedings



Eight conditions for lawful processing

Eight conditions for lawful processing

1. Accountability

2. Processing limitations

3. Purpose specification

4. Further processing limitation

5. Information quality

6. Openness

7. Security safeguards

8. Data subject participation

Eight Conditions for Lawful Processing

Responsible party is accountable for complying with measures which give effect to these conditions



(Can't contract out of obligations e.g., by outsourcing processing of information)

- Accountable from inception: at the time “purpose and means” determined
- Accountable throughout lifecycle of processing

Eight Conditions for Lawful Processing



Personal information must be processed:

- Lawfully
- In a reasonable manner that does not infringe privacy of data subject

Minimality:

- Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive

Eight Conditions for Lawful Processing

A responsible party may not process personal information.



Unless:

- Information – adequate, relevant and not excessive
- Data subject consents to the processing
- Processing is necessary for performance of a contract to which the data subject is party
- Processing complies with an obligation imposed by law
- Processing protects a legitimate interest of the data subject
- Processing is necessary – public law duty by a public body
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

Eight Conditions for Lawful Processing

Purpose
specification



Purpose:

- Personal information must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the responsible party
- Steps must be taken to make the data subject aware of the purpose of collection

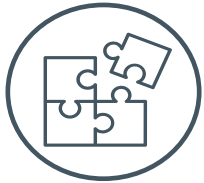
Right to be forgotten:

Personal information must not be retained longer than is necessary to achieve the purpose, subject to exceptions such as where:

- Required or authorised by law
- Reasonably required for lawful purpose
- Required by contract between parties
- Consent is given

Eight Conditions for Lawful Processing

Further processing
limitation



- Further processing must be 'compatible' with the initial purpose
- Various issues to consider to assess compatibility
- Various factors listed which will not be considered incompatible, e.g obligations for other legislation

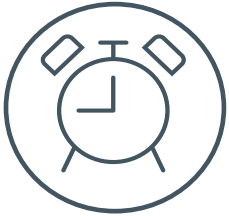
Eight Conditions for Lawful Processing



- Responsible party under duty to take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading, and updated where necessary
- Have regard to purpose for which personal information is collected or further processed

Eight Conditions for Lawful Processing

Openness



Timing: This awareness must be made:

- Before information is collected - if collected directly
- Before collection or as soon as reasonably practicable - other circumstances

Waiver:

- Data subject consents to non-compliance

Exceptions:

- Consent
- No prejudice to data subject legitimate interests
- Non-compliance is necessary to uphold the law or court decision
- Prejudice lawful purpose of collection
- Not reasonably practicable
- Information de-identified or used for historical purposes

At any time information is invited or entered, the data subject must be notified.

What are the practical implications for this requirement?

PAIA

Responsible Party must maintain documentation of its processing operations under its responsibilities according to PAIA (Section 14 or 51)

Eight Conditions for Lawful Processing

Integrity and Confidentiality of Personal Information

Security safeguards



Take appropriate, reasonable, technical and organisational measures to prevent:

- Loss, damage, unauthorised destruction
- Unauthorised access

In order to do this, responsible party must:

- Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control
- Establish and maintain appropriate safeguards against identified risks
- Regularly verify that safeguards are effectively implemented
- Ensure safeguards are regularly updated in response to new risks or deficiencies

Must have due regard to generally accepted information security practices and procedures:

- Generally
- Specific industry standards
- Professional rules and regulations

Eight Conditions for Lawful Processing

Notification of Security Compromises – What happens if there is a breach, or a suspected breach?



Where there are reasonable grounds to believe personal information has been accessed by an unauthorized person, the responsible party must:

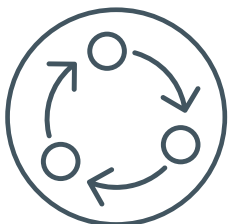
- Notify the Regulator
- Notify the data subject
- As soon as reasonably possible after the compromise
- May only delay if notification will impede a criminal investigation

How?

- In writing through letter, email, website, news media

Regulator may direct the responsible party to publicize the compromise.

Eight Conditions for Lawful Processing



Operator

- An operator, or anyone processing personal information on behalf of a responsible party or an operator, must:
 - Do so with knowledge or authorisation of the responsible party; and
 - Treat personal information as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

Written contract between operator and responsible party imposing security safeguards (audit of risks etc.)

Eight Conditions for Lawful Processing

Data subject
participation



Data subject is entitled to:

- Enquire – free of charge – whether his/her personal information being processed
- Request description of his/her personal information
- Request information on recipients of his/her personal information
- Challenge the accuracy of personal information
- Request correction of information (if inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully)
- Request deletion



Special personal information

Section 26 prohibits the processing of certain types of information such as, the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject except in certain circumstances.

Insurance industry processes personal information and special personal information.

Additional measures must be put in place/observed in relation to special personal information.



Processing special personal information

Responsible parties are prohibited from processing special personal information.



Exceptional conditions when special personal information may be processed:

- Processing is carried out with the consent of the data subject
- Processing is necessary for the establishment, exercise or defence of a right or obligation in law
- Processing is necessary to comply with an obligation of international public law
- Processing is for historical, statistical or research purposes and sufficient guarantees
- Processing requires disproportionate effort or appears impossible to ask for consent
- The information has deliberately been made public by data subject

Additional exceptions for specific categories of Special Personal Information



Information Officers

Who is the Information Officer?



- All private and public bodies must appoint an Information Officer
- Defined as the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act
 - CEO/equivalent officer/any person authorised by that officer; or
 - Person acting as such or any person duly authorised by such acting person

Who is a Deputy Information Officer?

Section 56

- Every private body must make provision, in the manner prescribed in section 17 of PAIA, with necessary changes, for the designation of:
- “Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of [POPIA]; and
- Any power or duty conferred or imposed on an information officer by [POPIA] to a deputy information officer of that ... private body.”

Duties and responsibilities of Information Officers



Section 55(1) duties include:

- The encouragement of compliance, by the company, with the conditions for the lawful processing of personal information;
- Dealing with requests made to the company pursuant to POPIA;
- Working with the Information Regulator in relation to investigations conducted pursuant to the prior authorisation provisions found under Chapter 6 of POPIA in relation to the company;
- Otherwise ensuring compliance by the company with the provisions of POPIA; and
- Any other duties and/or responsibilities as may be prescribed by the Information Regulator in terms of section 112(2)(d) of POPIA.

NB: Registration of Information Officers and Deputy Information Officers formally commenced on 1 May 2021.

Paper-based applications can be emailed to: registration.IR@justice.gov.za

Alternatively, delivered to: D House, 27 Stiemens Street, Braamfontein, Johannesburg 2001



Automated Decision Making

Section 71 of POPIA provides that a data subject may not be subject to a **decision which results in legal consequences** for him, her or it, or which affects him, her or it to a substantial degree, which is **based solely** on the basis of the **automated processing** of personal information **intended to provide a profile of such person** including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

UNLESS: the decision has been taken in connection with the **execution or conclusion of a contract** and:

- the requests of the data subject in terms of the contract are satisfied, or
- appropriate measures have been taken to **protect the data subject's legitimate interests**.
- Measures must provide an opportunity for a data subject to make representations about a decision.
- Responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information in order to allow data subject to make representations



Transborder information flows

Personal information may not be transferred to third party in a foreign country, **unless certain requirements are met:**

- RP must ensure that the Recipient of the information is subject to **law, binding corporate rules**, or **agreement** which provides **for 'adequate level of protection'** that:
 - Effectively upholds principles that are substantially similar to the conditions for lawful processing; and
 - Includes substantially similar provisions relating to the further transfer of personal information to third parties in foreign countries;
- NB - must obtain the **Consent** of data subject;
- Transfer must be **Necessary** for performance of contract between data subject and responsible party;
- Transfer must be Necessary for performance of pre-contractual measures at data subject's request;
- Transfer must be Necessary for conclusion or performance of contract concluded in the interest of data subject between responsible party and third party;
- Transfer must be For benefit of data subject, and:
 - Not reasonably practicable to obtain consent,
 - If it were, data subject would be likely to grant consent.





Prior Authorisation

Processing Activities requiring Prior Authorisation

Section 57. (1) - The responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing if that responsible party plans on –

1. Processing **Unique Identifiers** of data subjects - for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the information together with information processed by other responsible parties;
2. Processing information pertaining to the **criminal behaviour or on unlawful or objectionable conduct** on behalf of third parties.
3. Processing information for the purposes of **credit reporting**
4. Transferring **special personal information** or the **personal information of children to a third party in a foreign country that does not provide an adequate level of protection** for the processing of personal information.



Process of obtaining Prior authorisation



- Section 57. (1) "The responsible party **must obtain prior authorisation** from the Regulator, in terms of section 58, prior to any processing if that responsible party plans to – .
- Regulator must inform responsible party **within 4 weeks** whether or not it will conduct a more detailed investigation (s 58(3))
- Investigation period must not exceed **13 weeks** (s 58(4))
- Must **issue statement** concerning the lawfulness of the processing (s 58(5))
- Statement deemed to be an enforcement notice (s 58(6))
- Processing **deemed to be authorised if no response from Info Registrar** (s 58(7))

Date for enforcement of prior authorization provisions - 1 July 2021.



Security breaches

POPIA and security breaches



- As already discussed, one of conditions of lawful processing = security safeguards
- **Responsible parties/operators/anyone acting on their behalf** must ensure sufficient security safeguards are in place when processing
- Failure to do so = data breach = potentially disastrous
- Duty to blow the whistle on yourself once have reasonable grounds to believe:
 - Notify data subjects
 - Notify Information Regulator
- Do so as soon as reasonably possible after discovery (taking into account law enforcement and measures to restore integrity of system)
- Can only delay if law enforcement determines will impede a criminal investigation

Examples of Data Breaches



Cost of data breach report 2020: Poneman Institute and IBM



- Global average cost = **\$3.86 million = R67.5 million**
- South Africa = **\$2.14 million = R37 million**

Cost per record:

- United States = **\$242 = R4 230**
- South Africa = **\$155 = R2 700**

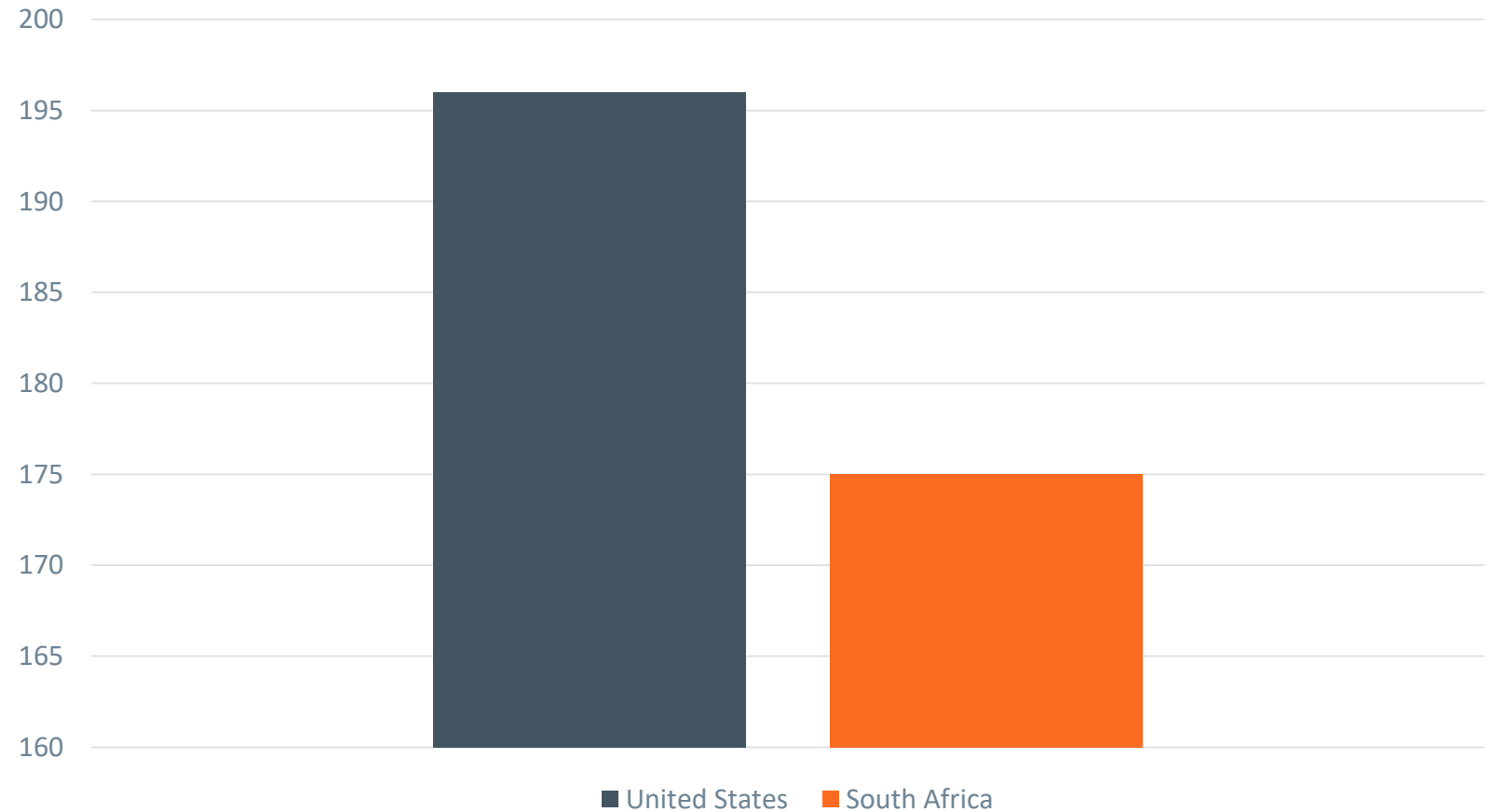
Average number of records per breach:

- United States = **32 434**
- South Africa = **22 060**

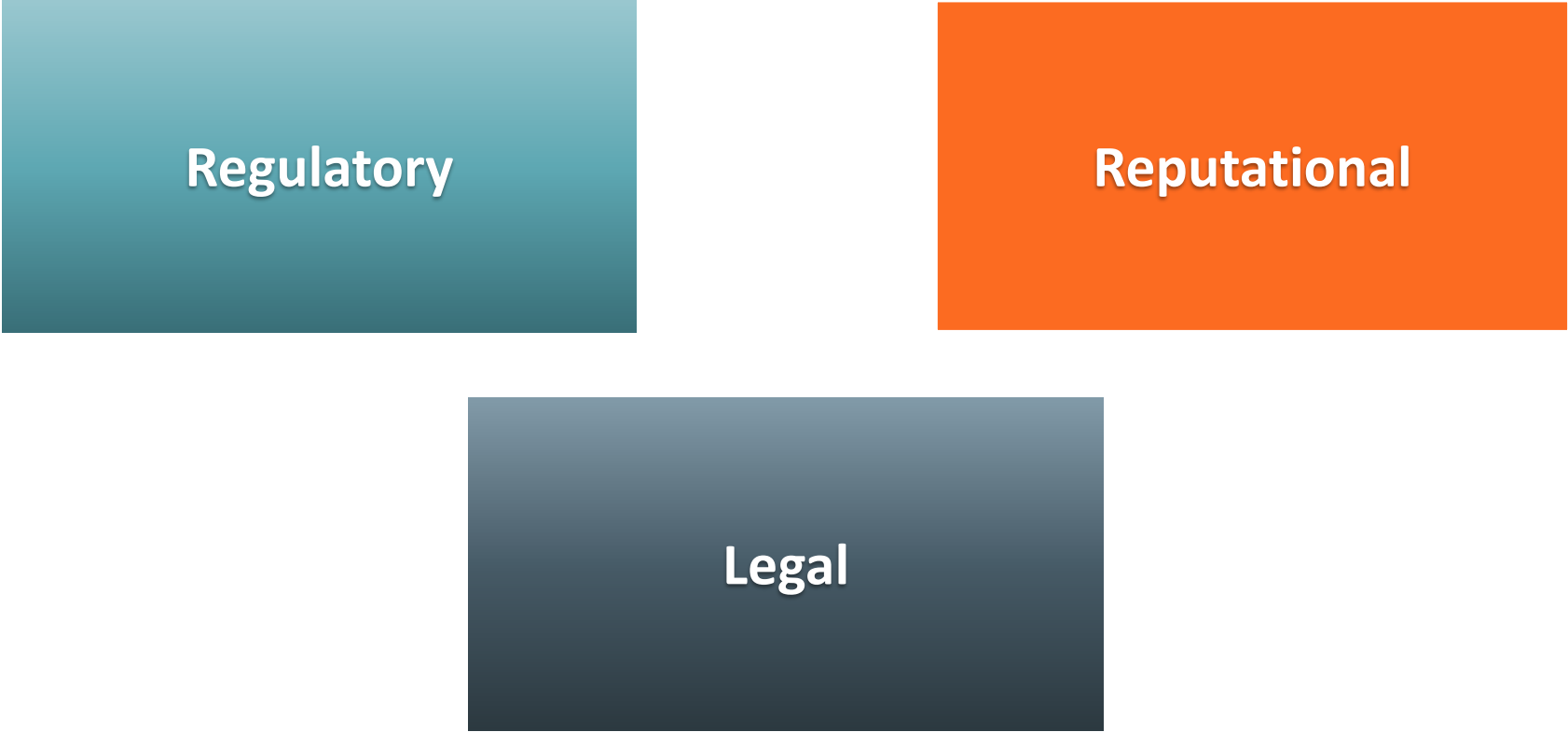


- United States = **196 days**
- South Africa = **175 days**

Average time taken to contain breach



Consequences of data breach



Regulatory

Reputational

Legal

Regulatory



Information regulator has the power to:

- **Enter and search** premises of responsible party
- Conduct private **interviews**
- **Summon and enforce** appearance of persons
- Compel written and oral **evidence**
- Adjudicate complaints by data subjects of breaches of personal information conditions



- Information regulator can:
- **Administer fines** of up to **R10 million** for failure to notify breach
- Damages (regardless of notification)

Administrative fines

Country	Date	Company	Fine	Reason given by the ICO
UK	2018	British Airways	Notice of intent – 183 million GBP	"People's personal data is just that - personal. When an organisation fails to protect it from loss, damage or theft, it is more than an inconvenience. That's why the law is clear - when you are entrusted with personal data, you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights"
UK	2019	Marriott	Notice of intent – 99 million GBP	'Failed to undertake sufficient due diligence' and could have 'done more to secure its systems'
UK	2017	Equifax	500 000 GBP	UK brand had failed to ensure that its parent company was protecting the data of its British customers.

Legal consequences



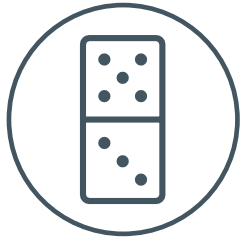
Reactive:

- **Damages** lawsuit from data subject or Information Regulator
- **Strict liability** for interference with **personal information** regardless of intention or negligence

Proactive:

- **Sue** IT supplier
- Sue hackers/fraudulent party /trace hackers and use Anton Piller application to obtain personal information
- Lay **criminal** complaint

Reputational consequences



- Customers will first **blame** company for breach
- Lost confidence
- Public **outcry**
- **Negative** media publicity
- Research shows up to **one-third** of consumers will stop doing business with organisations that have experienced a breach

Minimising reputational damage



- Crisis **communications strategy NB**
- Legal advisors part of media strategy
 - Court of law and court of public opinion
- **Engage** data subjects and Information Regulator
- Engage stakeholders (e.g., customers and shareholders)
- Engage public ? (e.g., SENS announcement)
- What happened, what are you doing about it, why it won't happen again

The GDPR

What is it?

When does it apply to you?

What do you need to do?





Questions?



www.webberwentzel.com

JOHANNESBURG

90 Rivonia Road
Sandton
Johannesburg, 2196, South Africa
T +27 11 530 5000



@WEBBERWENTZEL #WWEVENTS

CAPE TOWN

15th Floor, Convention Tower
Heerengracht, Foreshore
Cape Town, 8001, South Africa
T +27 21 431 7000



WEBBER WENTZEL #WWEVENTS

WEBBER WENTZEL

in alliance with > **Linklaters**