Thinking about POPI, a friend or foe?

WERKSMANS
ATTORNEYS

22 September 2020

Speakers

Ahmore Burger-Smidt

Director and Head of Data Privacy
aburgersmidt@werksmans.com

Jacques van Wyk

Director of Labour & Employment Practice
JvanWyk@werksmans.com

Neil Kirby

Director and Head of Healthcare & Life Sciences
NKirby@werksmans.com

Tracy-Lee Janse van Rensburg

Director of Banking & Finance
TJvRensburg@werksmans.com

Thin line between love and hate

Consent and Justification

WERKSMANS
ATTORNEYS

Ahmore Burger-Smidt

Director and Head of Data Privacy
aburgersmidt@werksmans.com

Lawful Processing

- At all stages and times based on at least one legal ground.

- Consent
- Contract
- Legal Obligation
- Data Subject Interests
- Public task
- Legitimate interest

LAWFUL - Compliant with laws and legal principles

Appropriate to the nature of the underlying relationship between the responsible party and the data subject

Lawful Processing and Data Subject Rights

		Right to Rectification	Right to Erasure	Right to Restriction	Right to Trans border Transfer	Right to Object
Consent	✓	✓	✓	✓	✓	Can withdraw consent
Contract	✓	✓	✓	✓	✓	x
Legal Obligation	✓	✓	x	✓	x	x
Data Subject Interests	✓	✓	✓	✓	x	x
Public Task	✓	✓	x	✓	x	✓
Legitimate Interests	✓	✓	✓	✓	x	✓

What did the drafters think?

Consent to infringement of privacy is a unilateral act. Therefore it may be revoked at any time preceding the defendant's injurious conduct. Consent can be given expressly or tacitly

In order to be valid, consent must meet certain requirements. Regarding the violation of privacy, it is particularly important that the consent must be voluntary. In addition, the consent must not be contrary to public policy or *contra bonos mores*

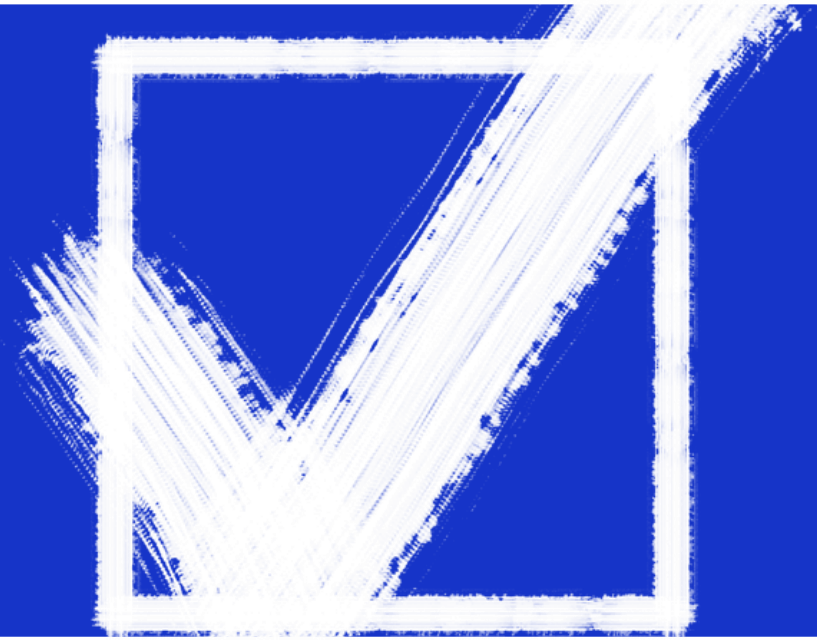
For this reason an irrevocable consent to violation of privacy is regarded as invalid

Thinking about consent

Clear	Clear, leaving no doubt or difficulty in understanding the purpose
Match	Enables a match between data subjects and responsible party's expectation
Available	Available in writing or orally
Comparison	Allows for comparison with subsequent processing purposes
Purpose	Allows to determine if the purpose does not correspond to the facts of the case

What can we learn from the GDPR?

"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"



We can learn from the cookies survey

The data subject must be able to withdraw consent as easily as they gave it

Companies should not ‘bundle’ consent for cookies with consent for other purposes, or with terms and conditions for a contract for other services provided

Companies should provide information about how data subjects can signify and later withdraw their consent, including by providing information on the action required for them to signal such a preference

Consent does not need to be given for each cookie, but it must be given for each purpose for which cookies are used

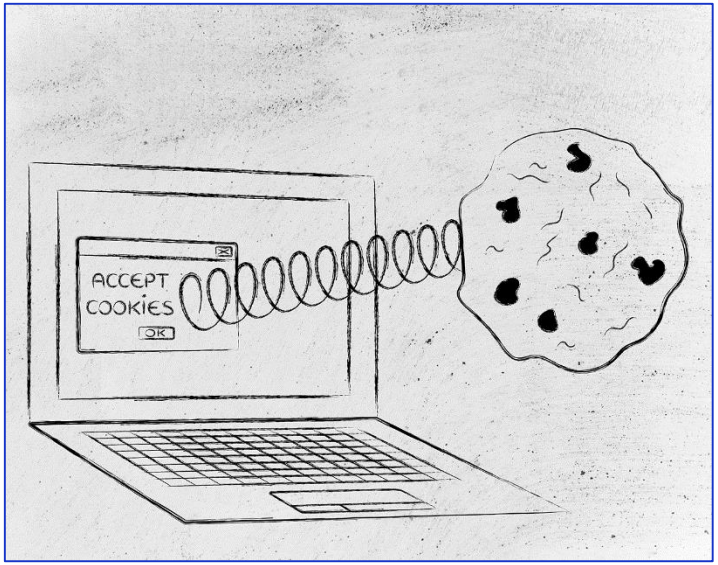
Pre-checked boxes and sliders - these do not comply with European law, as has been clarified in the Planet49 judgment of October 2019

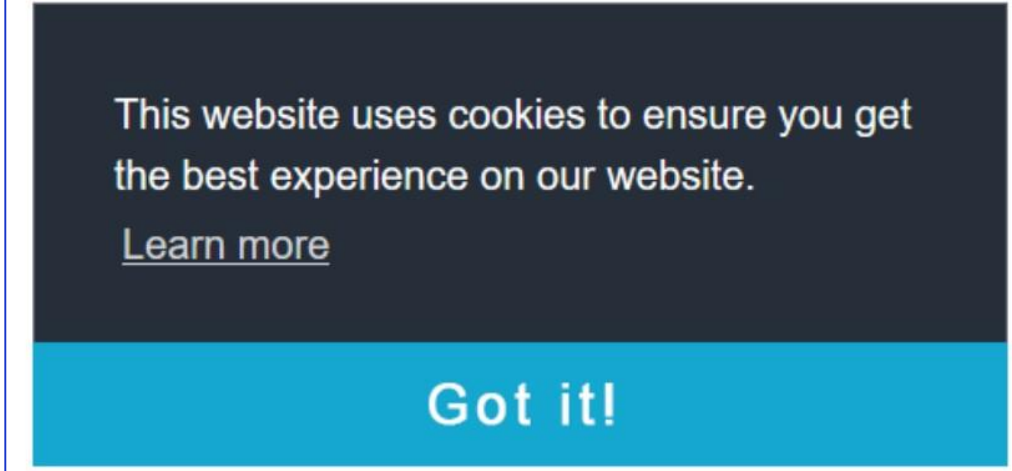
Clearly a problem

- Most websites with cookie banners had an interface that favoured an ‘accept’ option, without an option to ‘reject’ cookies

- Even where they did have an option to learn more about cookies, in many cases this did not include a layered option to accept or reject cookies by function

- A so-called ‘nudging’ approach to the web design is therefore common, with users effectively forced into accepting all cookies





The right to know

Wording in a cookie banner or notice which inform data subject that, by their continued use of the website – either through clicking, using or scrolling it - that a company will assume their consent to set cookies, is not permissible

If your processing involves personal data, you will need to meet the transparency requirements!

Conclusion

- ✓ The data subject's consent must be specific to each purpose for which a company are processing their data, it must be freely given and unambiguous and it requires a clear, affirmative action on the part of the data subject
- ✓ Silence or inaction by the data subject cannot constitute their consent to any processing of their data
- ✓ There is no such thing as obtaining consent by 'implication'

Questions?

From recruitment to dismissal

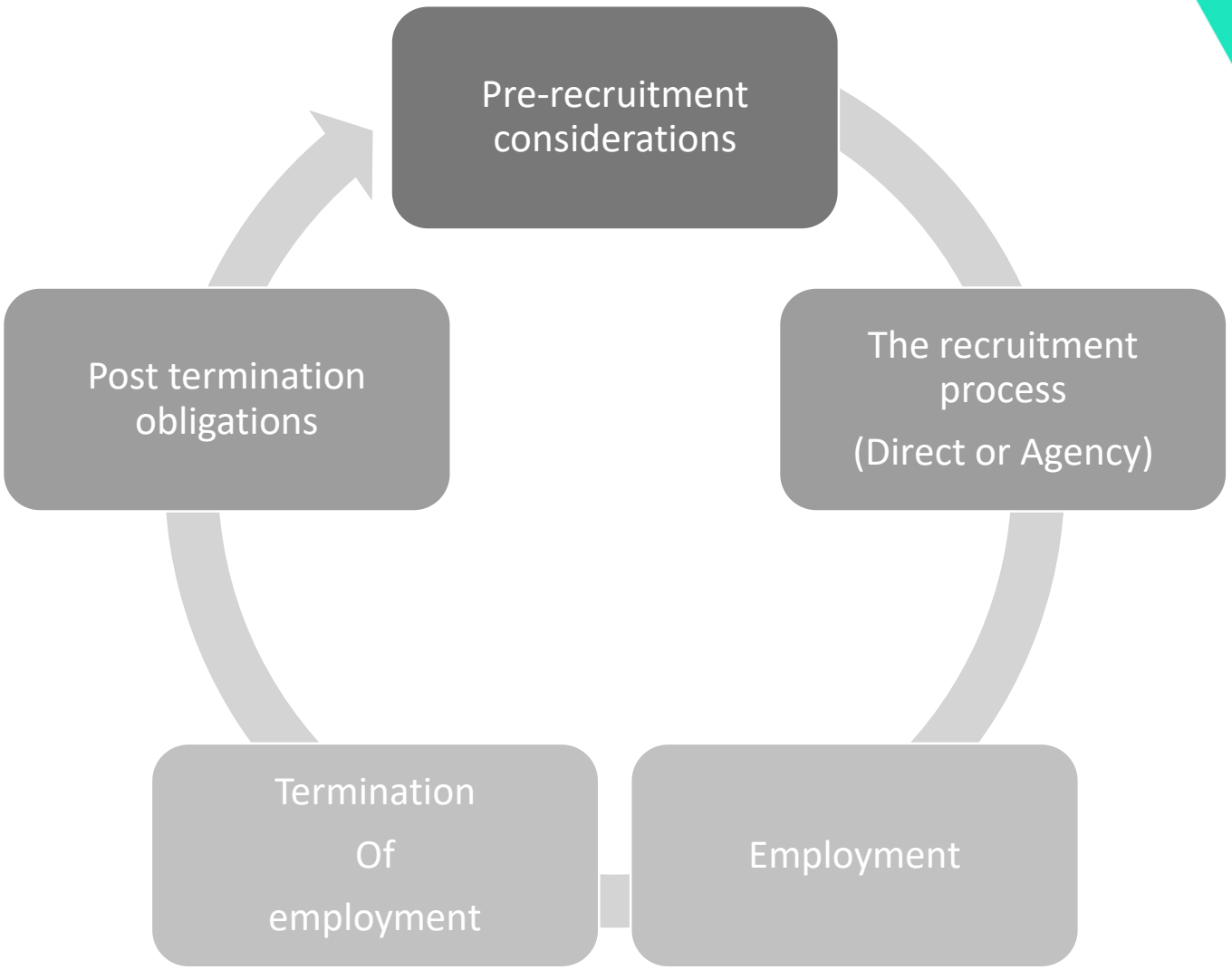
An employers obligations under POPIA

WERKSMANS
ATTORNEYS

Jacques van Wyk

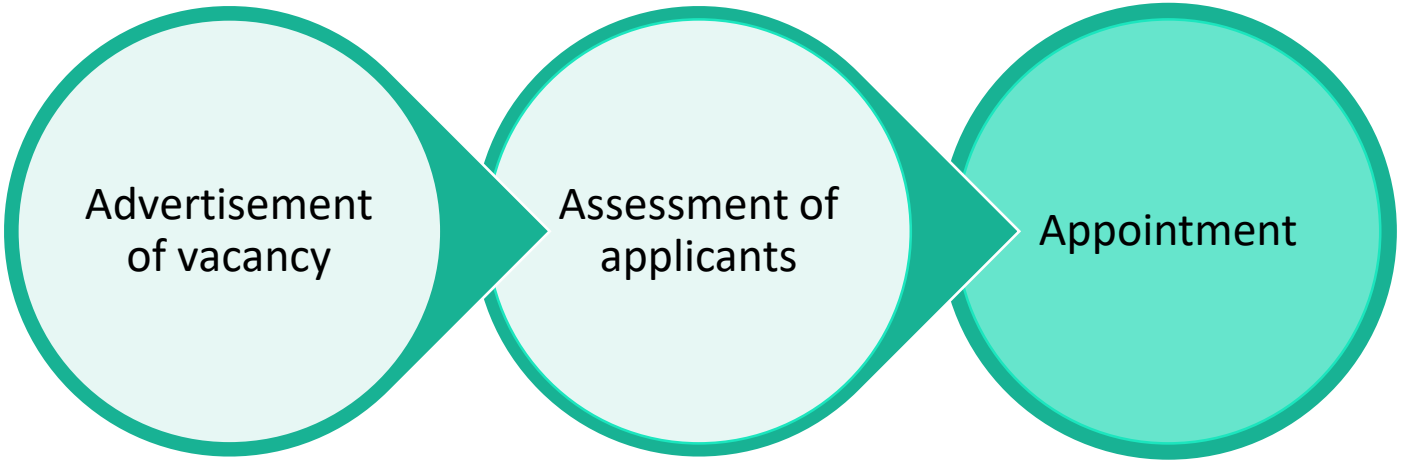
Director of Labour & Employment Practice
JvanWyk@werksmans.com

POPIA features throughout the employment lifecycle



Recruitment

Consideration and obligations at each stage

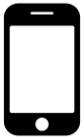


During employment

Various forms of personal information

Health status and medical claims

Travel records



Call records (on company provided phone or contract)

Company credit card purchases

Remuneration and bonuses

Union membership, union dues

Grievances, disciplinary sanctions, performance reviews, claims and/or disputes

Professional body memberships etc

Biometric information

Termination and Post Termination

Termination

- Reasons for dismissal
- Minutes/notes/documents/findings relating to the termination of employment
- Disputes about dismissal and outcome
- Remuneration and benefits as at the end of employment
- Tax directives
- Reference letters / Certificates of Service

Post Termination

- Employee's name, contact details, address and occupation;
- The time worked by an employee;
- The remuneration paid to the employee;
- Reason for termination; and
- Employee benefit schemes – beneficiary details; payments to them etc. marital status, exclusions of pre-existing conditions etc.

Next time – Case Study

ABC is a multinational company with local offices in the Western Cape.

Employees access the office by means of their thumbprint.

ABC's business is the processing of credit information on behalf of customers.

ABC makes use of a company to recruit its employees, Recruitment Pty Ltd.

ABC stores the majority of its information digitally using a cloud based systems, whose servers are located in Norway.

ABC is a 'designated employer' for the purposes of the Employment Equity Act.

Questions?

POPIA Webinar: The how, why and what of the information Officer

WERKSMANS
ATTORNEYS

Neil Kirby

Director and Head of Healthcare & Life Sciences
NKirby@werksmans.com

The Information Officer

The Information Officer and the Private Body

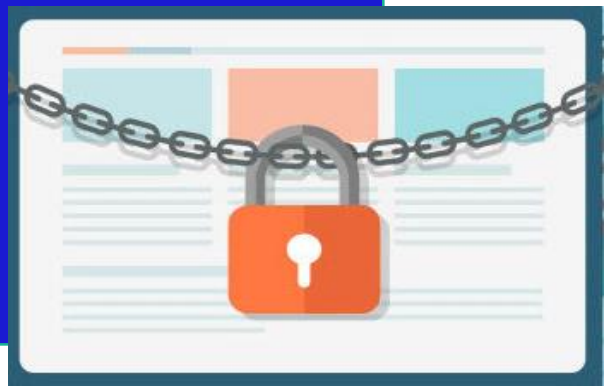
Section 55 of POPIA

Regulation 4 of the Regulations under POPIA

The Information Officer

Origins

- "Head of a private body" (section 1 of the Promotion of Access to Information Act No. 2 of 2000) or a person delegated by him/her
- International co-ordination of information policy
- Defined roles and responsibilities
- Knowing what you don't know
- Information assessment
- Historically, a statutorily passive role
- "Setting a watchman"



The Information Officer

Of Encouragement

The Information Officer

BEFORE WE GET CARRIED AWAY:
Information landscape in the current age
(section 23 of POPIA)

- "About the Data Subject"
- Special personal information
- Grounds of refusal – PAIA
- Health records - PAIA

The Information Officer

CASE LAW: AN INTEGRATION NOT A MODIFICATION

- **Assessing a request – section 50(1) of PAIA**
- **Meeting the criteria – exercise or protection of a right: POPIA**
- **"required for the exercise or protection of any rights"**
- **A fact based enquiry, "[i]t involves something more than that the information would be of assistance, which is a minimum threshold requirement"** (*Mahaeeane and another v Anglogold Ashanti Ltd* [2017] 3 All SA 458 (SCA) at para. 13) **and "I think that 'reasonably required' in the circumstances is about as a precise formulation as can ever be achieved, provided that it is understood to connote a substantial advantage or an element of need."** (*Clutchco (Pty) Ltd v Davis* 2005 (3) SA 486 (SCA))

Questions?

Security Safeguards and Cybersecurity -

Data Breaches

WERKSMANS ATTORNEYS

Tracy-Lee Janse van Rensburg

Director of Banking & Finance
TJvRensburg@werksmans.com

Introduction

Data breaches and cyber attacks are fast becoming a common and frequent threat to businesses in South Africa.

Data breaches can include

- Erroneously sending emails or documents
- Theft of devices
- Phishing attacks
- Cyberattacks

Business interruption

Financial hardships

Reputational implications

Regulatory sanctions - Information Regulator (Complaint and investigative process, administrative fines and referral to Enforcement Committee)

Civil remedies

Data Security

Obligation to secure the integrity and confidentiality of personal information in possession or under control by taking appropriate and technical measures to prevent unlawful accessing and processing of information and loss of personal information

Identify all reasonably foreseeable risks

Establish safeguards

Regular verification of safeguards

Take cognisance of accepted information security safeguards/practices generally applicable

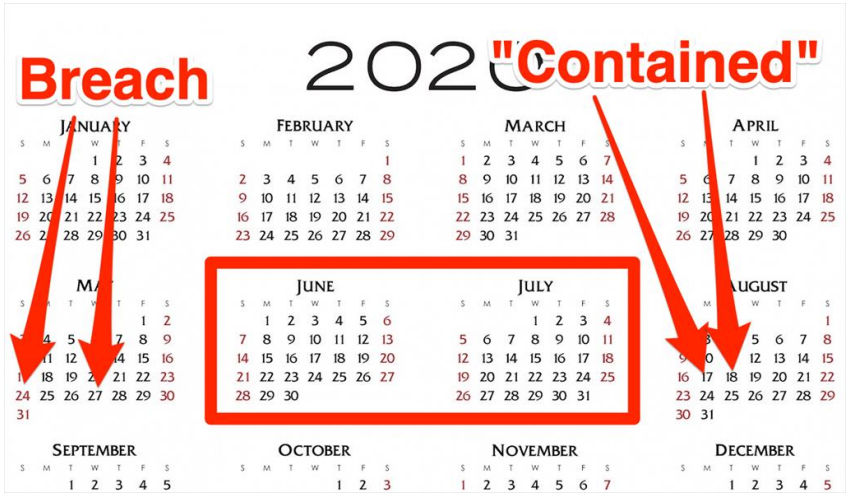
No one size fits all approach

Develop a clear and effective incident report plan	Test internal response processes and implement processes to minimise risk after a breach	Identify processes to notify partners of the breach (including notification to the Information Regulator).	Periodic test runs of incident report plan	Training and awareness of staff on incident report plan	Know where risks are

Examples of Data Breaches

Experian

- Personal information of 24 million South Africans and almost 800,000 businesses
- Initially Experian advised no consumer credit or consumer information was obtained
- Discovered information disclosed included phone numbers, id numbers, employment details, banking details
- Information was dumped on Swiss regulated website "We-Sendit"
- Breach occurred in May 2020, discovered 22 July 2020, Information Regulator informed 06 August 2020, formal report was made 14 August 2020, Anton Piller executed 18 August 2020.



Information Regulator

- is conducting an independent review to assess the extent of the data breach and to explore a suitable solution to protect information disseminated
- will notify Federal Data Protection and Information Commissioner and its counterpart in Switzerland
- Advised public that the grace period provided for in POPIA does not absolve responsible parties from the legal obligation of ensuring that they process personal information *"in accordance with POPIA"*

Examples of Data Breaches

Lifehealthcare Group

- Was a victim of cyberattack in the midst of COVID-19 in June 2020
- Did not reveal nature of the breach but it did make a voluntary announcement
- External cyber-security experts and forensic teams called in
- Systems were taken offline to contain the attack (admissions, business processing, email)
- Switched over to "back-up manual processing systems".

Momentum Metropolitan

- 3rd Party unlawfully accessed a limited portion of data of a subsidiary of the Group
- Awareness on 13 August and immediately activated its IT security incident plan
- Additional system monitoring
- No client or member data released

Garmin

- September 2019 clients credit card information hacked
- July 2020 second breach but no customer data or payment information accessed or stolen
- Delays in information being processed

Implications for South Africa

IBM Security study revealed that data breaches are costing South African companies R40.2 million per breach, on average among the companies studied

Attacks on customer, employee and corporate data most prevalent and the costliest causes of breaches.

Average time to:	South Africa	Global
Identify data breach	177 days	207 days
Contain data breach	51 days	73 days

- Root causes data breaches
  - Human error – 26%
  - System glitches – 26%
  - Malicious/criminal attack 48%
- Investments in smart technology resulted in lower breach costs (quicker to investigate, isolate, contain and respond to and reduces financial and reputational impact), cost saving of R2.5 million.
- Incident report preparedness imperative. Need for a team and plan (which are regularly tested), cost saving of R3.4 million
- Remote working will have a cost to companies due to less controlled environment

Questions?

WERKSMANS
ATTORNEYS

Thank you

22 September 2020

Presentation and recording will be made available on request**.**

Keep us close