

Deloitte.

Protection of Personal Information POPI compliance.



Protection of Personal Information
4 May 2010
SAPA

History of the POPI Bill

- ✓ In October 2005 the Law Commission finalised its investigation into the status of privacy protection in SA
- ✓ The Commission found that privacy law was lacking regardless of the Right to Privacy in the Constitution
- ✓ The Commission recommended a new and separate law to deal with the protection of personal information
- ✓ After the review of more than 5000 submissions on the original text of the Bill, a revised version was approved by cabinet during August 2009
- ✓ The Protection of Personal Information Bill 2009 is now heading for approval by Parliament and the National Council of Provinces
- ✓ Possible date of enactment – September 2010 – 1 year implementation

Aims of the POPI Bill

- ✓ To give legislative effect to Right to Privacy contained in section 14 of the Constitution – effective protection of personal information
- ✓ To specifically regulate the matters of unsolicited electronic communications and automated decision making
- ✓ To regulate the cross border flow of PI

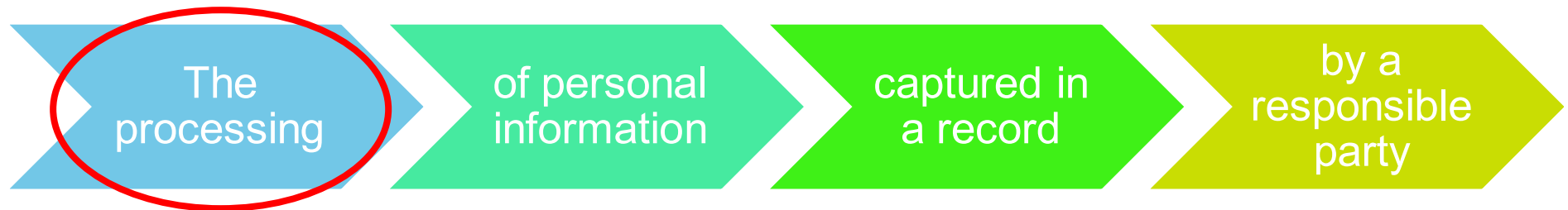
Scope of application

In terms of section 3 the Bill applies to the following:



Scope of application

In terms of section 3 the Bill applies to the following:

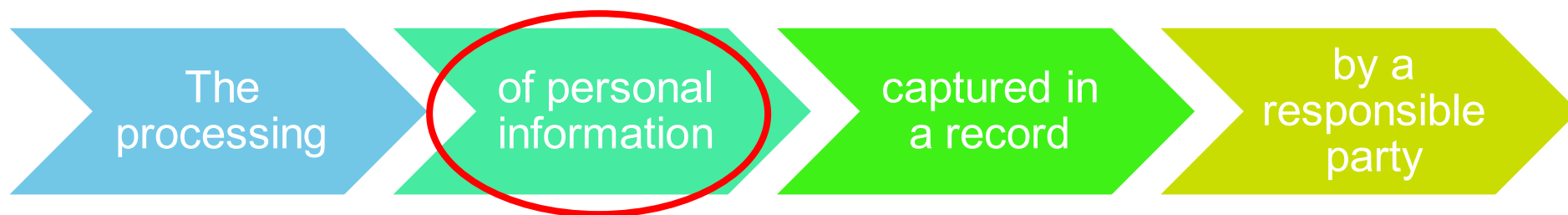


“**processing**” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

- (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- (b) dissemination by means of transmission, distribution or making available in any other form; or
- (c) merging, linking, as well as blocking, degradation, erasure or destruction of information;

Scope of application

In terms of section 3 the Bill applies to the following:

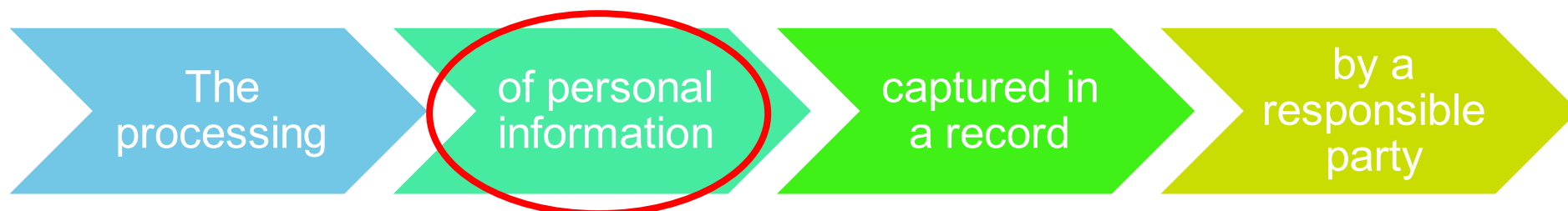


“personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

- (a) information relating to the 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 of the person;
- (b) information relating to the education or the medical, financial, criminal or employment history of the person;
- (c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
- (d) the blood type or any other biometric information of the person;
- (e) the personal opinions, views or preferences of the person;

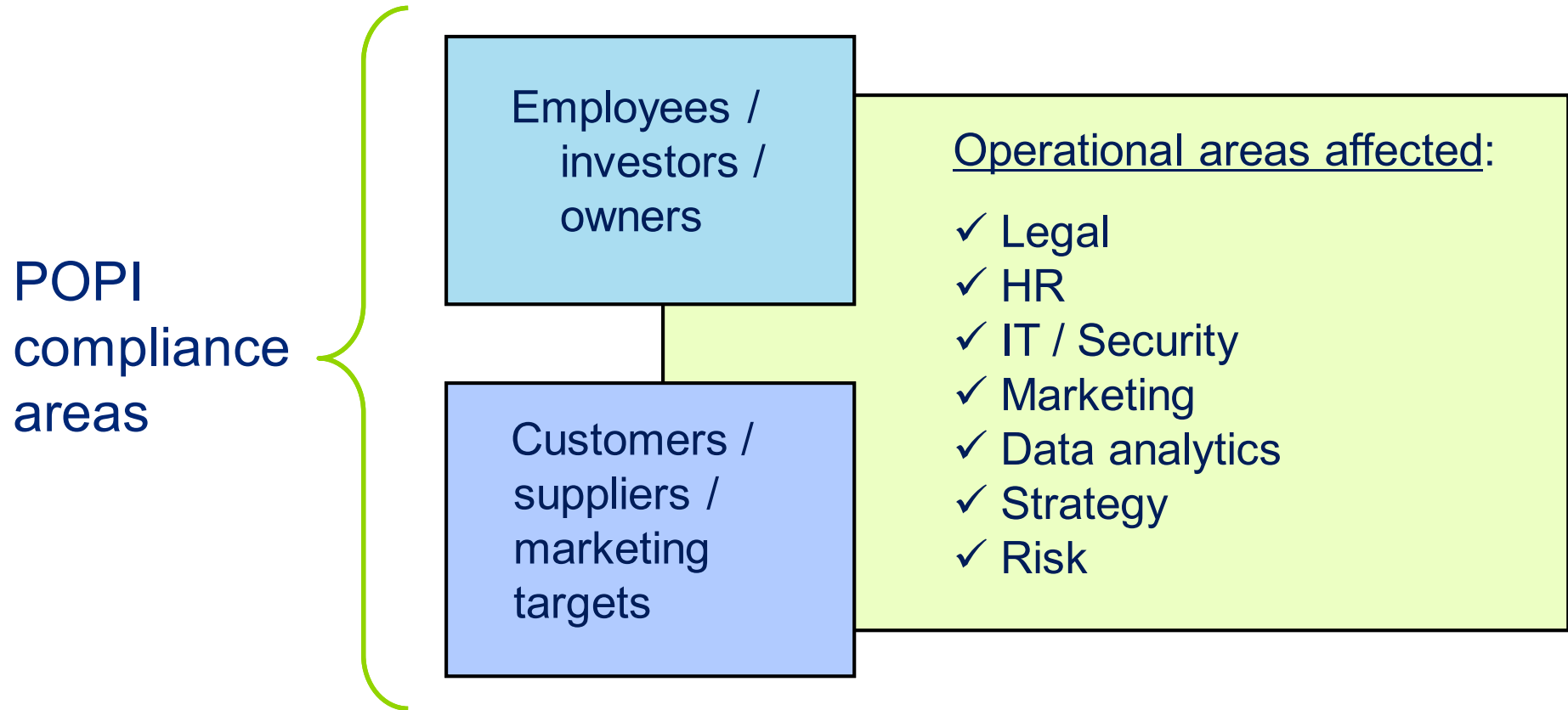
Scope of application

In terms of section 3 the Bill applies to the following:



- (f)* correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g)* the views or opinions of another individual about the person; and
- (h)* the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

Application of POPI to your business environment



Your duties and obligations

Principle 1: Process PI in accordance with the Bill

Principle 2: Collect PI from DS, with consent, for a specific, explicit and lawful purpose

Principle 3: Retain PI for a reasonable period, then destroy it

Principle 4: Process PI according to the stated purpose of collection

Principle 5: Ensure that PI remains complete and accurate

Principle 6: Notify the data subject and the regulator that you are processing PI

Principle 7: Protect the security and integrity of PI

Principle 8: Comply with operator requirements

Principle 9: Facilitate DS report on PI held and allow for correction or deletion requests

Operator provisions

“operator” means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party

Rule A – Operator to process with RP knowledge and authorisation

Rule B – Operator to treat PI as confidential and must not disclose it

Rule C – RP to ensure operator establishes and maintains the legislated security

Rule D – Written contract required (including confidentiality and security)

Other provisions of the Bill

- ✓ Establishment and duties of the Regulator
- ✓ Appoint Information Officer
- ✓ Trans-border information flow
- ✓ Prevention of spam (unsolicited communications)
 - Only allowed with prior consent
 - If recipient is an existing client or customer



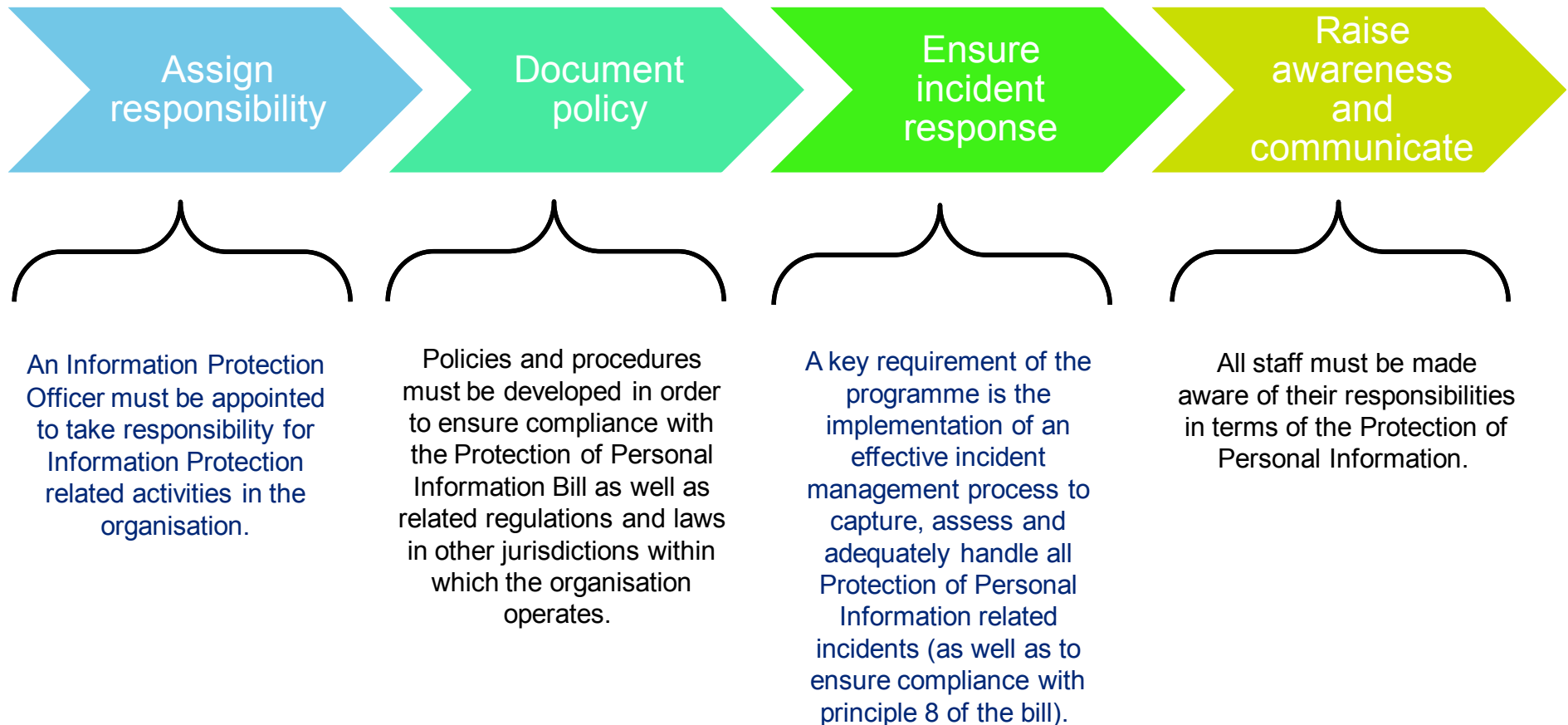
Remedies for non-compliance

- ✓ Lodgement of complaints with the Regulator
- ✓ Information notice for audit report
- ✓ Enforcement notice
- ✓ Civil damages claims
- ✓ Criminal prosecution (fines and imprisonment)



Our recommended “Quick Start” response...

To enable you to take proactive steps toward reaching compliance with the Bill, we have formulated the following approach:



Deloitte.

Records and Email Management.

Records and Email Management
4 May 2010
SAPA



Records Management
Why keep records
and emails?

Why retain records and emails?

Businesses retain records and emails for four main reasons:

- ✓ Operational reasons
- ✓ Legislative compliance – no less than 25 laws of general application prescribe the retention of certain records for certain periods in certain formats
- ✓ In industries like financial services, health, retail, mining, insurance and energy there are further specific retention laws
- ✓ Evidence

Why retain records and emails?

General laws that prescribe the retention of business records include the following:

- ✓ Companies Act
- ✓ Income Tax Act, VAT Act, Customs & Excise Act
- ✓ Labour Relations Act, Employment Equity Act, Basic Conditions of Employment Act
- ✓ National Credit Act
- ✓ Consumer Protection Act
- ✓ Promotion of Access to Information Act
- ✓ Electronic Communications & Transactions Act
- ✓ Regulations of Interception of Communications Act

Records Management Electronic retention

Electronic retention

The electronic retention of documents and records are governed by section 16 of the ECT Act:

16. Retention.—(1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if—

- (a) the information contained in the data message is accessible so as to be usable for subsequent reference;
- (b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- (c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in [subsection \(1\)](#) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Electronic evidence

The electronic evidence is governed by section 15 of the ECT Act:

15. Admissibility and evidential weight of data messages.—(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence—

- (a) on the mere grounds that it is constituted by a data message; or
- (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to—

- (a) the reliability of the manner in which the data message was generated, stored or communicated;
- (b) the reliability of the manner in which the integrity of the data message was maintained;
- (c) the manner in which its originator was identified; and
- (d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Records Management Risks of non- compliance

The risk of non-compliance

- ✓ Criminal fines and civil liability
- ✓ No or worthless electronic evidence
- ✓ Inability to conduct disciplinary hearings
- ✓ Poor corporate governance regarding records
- ✓ Ignoring potentially more effective / cheaper way of doing business
- ✓ Limited security / access control

Records Management Recommendations

E-mail and records management recommendations:

- ✓ Conduct a health check on your existing technology infrastructure to determine levels of legal compliance and adequacy for business requirements
- ✓ Conduct similar health check on future technology acquisitions
- ✓ Adopt a records management policy
- ✓ Adopt an email archiving policy
- ✓ Adopt electronic evidence policy
- ✓ Adopt and update **records retention schedules** (detailing all relevant retention legislation, records subject to retention requirements, retention periods and formats)

Benefits of a good records management system:

