



Camargue

Specialised Liability Management

**PROTECTION**

OF

**PERSONAL INFORMATION ACT**

## Protection of Personal Information Act

Copyright © 2015 Camargue and Kirsty Melville-Nieman



**Camargue**

Specialised Liability Management

No part of this book may be reproduced or utilised in any form or by any means, electronic, mechanical, or other means, including photocopying and recording, or other information storage or retrieval system, without permission from the author.

eISBN: 978-0-620-66207-9

Cover & Layout design:

Designwave

[www.designwave.co.za](http://www.designwave.co.za)



**This guide should not be seen as a substitute for legal advice. If you require particular information you are advised to consult with a qualified lawyer. While every care has been taken to ensure the information in this book is accurate at the time of going to print, the publisher, Camargue Underwriting Managers, and author, Kirsty Melville-Nieman, may not be held liable for any error or loss suffered as a result.**

**© 2015 Kirsty Melville-Nieman and Camargue Underwriting Managers**



Camargue

Specialised Liability Management

# PROTECTION

---

OF

---

# PERSONAL INFORMATION ACT



# CONTENTS

<b>Chapter 1</b>	1
<b>Introduction</b>	1
Background	2
Purpose	3
The need	3
Application of the Act	4
Interpretation	5
Exclusions	5
<i>Journalistic, literary or artistic purposes</i>	6
Exemptions	7
Implementation	9

# Chapter 2 \_\_\_\_\_ 10

## Important definitions \_\_\_\_\_ 10

Responsible party _____	11
Public and private bodies _____	12
Types of personal information _____	13
Data subjects _____	14
Data subject's rights _____	15
Data processing _____	16

# Chapter 3 \_\_\_\_\_ 18

## Conditions for lawful processing \_\_\_\_\_ 18

1. Accountability _____	19
2. Processing limitation _____	20
3. Purpose specification _____	23
4. Further processing limitation _____	26
5. Information quality _____	27
6. Openness _____	28
7. Security safeguards _____	30
8. Data subject participation _____	30

# Chapter 4 \_\_\_\_\_ 34

## Security safeguards, data breaches and liability \_\_\_\_\_ 34

Cyber-crime _____	35
Types of data breaches _____	38
<i>eBay's data breach examined</i> _____	40
Identity theft _____	43
<i>Dangers of data breaches to consumers</i> _____	43
<i>Operators</i> _____	44



Potential liability under POPI	45
Cyber liability insurance	46
Camargue's cyber liability cover	47

## Chapter 5 49

### Processing of special personal information 49

General authorisation	50
Prior authorisation	51
Exemptions	52
<i>Authorisation concerning a data subject's religious or philosophical beliefs</i>	52
<i>Authorisation concerning data subject's race or ethnic origin</i>	52
<i>Authorisation concerning a data subject's trade union membership</i>	53
<i>Authorisation concerning a data subject's political persuasion</i>	53
<i>Authorisation concerning a data subject's health or sex life</i>	54
<i>Authorisation concerning a data subject's criminal behaviour or biometric information</i>	56

## Chapter 6 57

### Processing of personal information of children 57

## Chapter 7 59

### Direct marketing, directories and automated decision making 59

Direct marketing by means of unsolicited electronic communications	59
Directories	61



Automated decision making	62
---------------------------	----

## Chapter 8

<b>Penalties and enforcement</b>	64
Information Regulator	64
Complaints	65
Penalties	66
Offences	66
Administrative fines	67
Civil action for damages	68
<b>Appendix I</b>	70
<b>Appendix II</b>	74
<b>Appendix III</b>	78
<b>Appendix IV</b>	86

## TABLE OF FIGURES

Figure 1 Definition of responsible party	11
Figure 2 Definition of public and private bodies	12
Figure 3 Definition of personal information	13
Figure 4 Definition of processing	16
Figure 5 Conditions for lawful processing of personal information	19
Figure 6 Frequency of incident classification patterns (Verizon Enterprise Solutions, 2013)	38
Figure 7 Screen capture of the password update request on eBay.com	78





# Chapter 1

## INTRODUCTION

More than a third of South Africa's companies have experienced data breaches according to Kaspersky Lab, an international information technology security provider.<sup>1</sup> Such data breaches can result in not only millions of rands of damages for companies but also risk exposing consumers' personal information – opening them up to [identity theft and fraud](#). In 2014, 974 million company records were lost or stolen in South Africa – which is 31 records every second.<sup>2</sup>

---

1 <http://www.news24.com/Technology/News/SA-firms-lose-data-in-software-breaches-20140115>

2 <http://www.fin24.com/Tech/Companies/Cybercrime-costs-SA-firms-billions-20150320>

Furthermore, these stolen records lead to losses of at least R5.8 billion for South African businesses.

The Protection of Personal Information Act (POPI) is South Africa's first piece of legislation to solely address data privacy issues. The Act has been closely modelled on the European Union's Data Protection Directive which will in turn make it easier for European companies to do business within the Republic. While POPI directly addresses data privacy and processing, previous legislation has helped to pave its way. [The Electronic Communications and Transactions Act of 2002](#) contains two sections on the protection of personal information, namely the scope of protection of personal information (Section 50) and the principles for electronically collecting personal information (Section 51). These provisions, however, are only voluntary and relate to personal information that has been obtained through electronic transactions. These provisions will be repealed once POPI comes into effect.

## BACKGROUND

The Protection of Personal Information Bill was developed out of a necessity to protect the vast amount of [personal information](#) being processed, stored and transferred by [responsible parties](#) within the Republic. The Bill further sought to establish minimum requirements around such processing. POPI follows an investigation by the South African Law Reform Commission into privacy and data protection which was first released for comment in 2005.

The Bill was tabled in Parliament in August 2009 and was signed into law by President Jacob Zuma on 26 November 2013 (after being passed by the National Assembly in August 2013). Once the Act (a Bill becomes an Act once it is signed by the President) comes into effect, South Africa's data protection regulation will be in line with international standards.



While The Act has been enacted, President Zuma is yet to announce the [commencement date](#). This will be done by way of notice in the Government Gazette.

## PURPOSE

As with any piece of legislation, this Act has very specific purposes that its requirements aim to achieve. One such purpose is to uphold the constitutional right to privacy (which is enshrined in section 14 of the [Constitution of South Africa 1996](#)) by means of protecting an individual's personal information. This right to privacy must, however, be balanced against other rights such as the right to access to information and free flow of information. The Act will regulate every aspect of the processing of personal information, from its collection to its destruction and everything in between such as storage and safeguarding. It will also provide persons with recourse should their personal information not be processed in the prescribed manner. This recourse will be in the form of an [Information Regulator](#) to be established in accordance with the Act.

## THE NEED

Over the past two decades, Information Technology has developed significantly and has become an indispensable part the way business is conducted. However, it has also brought with it new risks and challenges that need to be overcome by organisations as well as individuals in order to protect against cyber exposures and liability.



One such example is the Internet which has given criminals the ability to “break-in” and steal information stored on computer networks thousands of kilometres away or remotely install malicious viruses. The implication of such threats is discussed in detail in [Chapter 4](#).

The Protection of Personal Information Act therefore arose out of a need to protect the large volumes of personal information that flows through the Republic every day by ensuring minimum standards of safeguarding and processing this information.

The impact of this legislation will be far-reaching and will significantly affect the way that companies collect, store, use and disseminate personal information.

## APPLICATION OF THE ACT

The Act will apply to the processing of personal information recorded by automated and non-automated means in order to form part of a filing system (i.e. POPI will apply whether the documents are in a digital format or paper documents in a filing cabinet). This includes all companies domiciled (having a principal place of business) within the Republic as well as those domiciled elsewhere that make use of automated or non-automated means of processing personal information within the Republic. Companies that are not domiciled within the Republic that use automated or non-automated means only to forward personal information through the Republic are excluded from compliance.



# INTERPRETATION

Where any other piece of legislation provides more extensive conditions for lawfully processing personal information, those extensive conditions will prevail. The Act must be interpreted in a manner that will give effect to the purpose of the Act but that does not prevent a public or private body from exercising or performing its powers, duties or functions in terms of the law.

# EXCLUSIONS

The Act does not apply to the processing of personal information in the course of a purely personal or household activity. Therefore the manner in which you store and process your own personal information is entirely up to you. If you were to run a business from home, however, you would be deemed a data processor and would need to ensure complete compliance with the Act.

Personal data that has been de-identified so that it cannot be re-identified again is also not covered by the Act. To de-identify a [data subject's](#) personal information means to delete any information that identifies the data subject, or which can be linked or manipulated to identify the data subject.

Public bodies, or anyone working on their behalf, are exempt from the requirements of the Act when processing personal information that involves national security. This includes activities that aim at assisting in the identification of the financing of terrorists and related activities, defence or public safety as well as preventing, detecting and combating money laundering. However, [safeguards](#) still need to be in place to ensure the protection of such personal information.



Cabinet, its committees and the Executive Council of a province are all exempt from the Act's requirements. Processing of personal information relating to the judicial functions of a court or for investigating or prosecuting an offender is also exempt.

## Journalistic, literary or artistic purposes

Further exclusions are granted for journalistic, literary or artistic purposes. However this is only to the extent that such exclusion is necessary to reconcile the right to privacy with the right to freedom of expression as a matter of public interest. For example, a journalist who is investigating a corrupt government official would not have to follow the requirements of this Act when sourcing or processing the official's personal information as exposing the corrupt official would be in the public's interest.

Fears have been expressed as to whether the ultimate effect of the Act will have on the freedom of press.<sup>3</sup>

Where personal information is processed for journalistic purposes, the responsible party's code of ethics will apply to the processing so long as the code provides adequate safeguards for protecting the personal information. In order to determine whether the code's safeguards are adequate, the following must be considered:

- ▶ The special importance of the public interest in freedom of expression;
- ▶ Domestic and international standards, balancing the-
  - ▷ public interest in allowing for the free flow of information to the public through the media (right of the public to be informed);

---

3 <http://www.archivalplatform.org/blog/entry/popia/>



- ▷ public interest in safeguarding the protection of personal information of [data subjects](#).
- ▶ The need to secure the integrity of personal information;
- ▶ Domestic and international standards of professional integrity for journalists;
- ▶ The nature and ambit of self-regulatory forms of supervision provided by the profession.

Any responsible party that processes personal information for journalistic, literary or artistic purposes would do well to re-assess their code of ethics in terms of this Act and ensure that its provisions are strengthened and that safeguards are substantial.

## EXEMPTIONS

The [Regulator](#) may grant a responsible party an exemption to process personal information, even if the processing is in breach of a [condition](#) for the processing of such information. This must be done by way of a notice in the *Gazette* and after the Regulator is satisfied that:

- ▶ There is a public interest in the processing that outweighs the interference with a data subject's privacy;
- ▶ There is a clear benefit to the data subject or a third party that outweighs the interference with their privacy.



Public interest is given to mean:

- ▶ The interests of national security;
- ▶ The prevention, detection and prosecution of offences;
- ▶ Important economic and financial interests of a public body;
- ▶ Fostering compliance with legal provisions established in the interests referred to above;
- ▶ Historical, statistical or research activity; or the special importance of the interest in freedom of expression.

Where personal information is processed for the purpose of discharging a relevant function, it is exempt from the following sections of the Act - :

Section 11: Consent, justification and objection

Section 12: Collection directly from data subject

Section 15: Further processing to be compatible with purpose of collection

Section 18: Notification to data subject when collecting personal information

- to the extent to which the application of those provisions to the personal information would likely prejudice the proper discharge of the function.

A relevant function is any function of a public body or any function that is conferred on any person in terms of the law which is performed with the aim of protecting members of the public from financial loss or improper conduct.



# IMPLEMENTATION

Once the date of commencement of the Act has been published in the Gazette, responsible parties will have a period of **one year** from this date in which to implement the Act. The minister may extend this period to a period not exceeding three years, either on request, on his/ her own accord or after consultation with the Regulator.

However, there are some sections of the Act that are already in effect as a result of a proclamation signed by the president and gazetted on **11 April 2014**.<sup>4</sup> The following sections came into effect on the day of the proclamation:

**Section 1:** Definitions in the Act

**Part A of Chapter 5:** the establishment of an [Information Regulator](#), the powers, duties and functions of the Regulator, appointment and terms of office of members of the Regulator, appointment of staff and the chief executive officer.

**Section 112:** Minister may make Regulations relating to the establishment of the Regulator and that the Regulator may make Regulations in terms of certain areas.

**Section 113:** Procedures for making Regulations by the Minister and the Regulator.

Ignorance of the Act is not a valid defence for violating its conditions. It is important that responsible parties act early in aligning their policies and practices with the requirements of the Act as doing so will require a significant amount of time and effort.

**The Act will apply to all personal information that is in your possession prior to the Act's commencement date. This includes not only personal information that is stored in digital format, but also information stored on other mediums such as papers in a filing cabinet.**

---

4 <https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx>

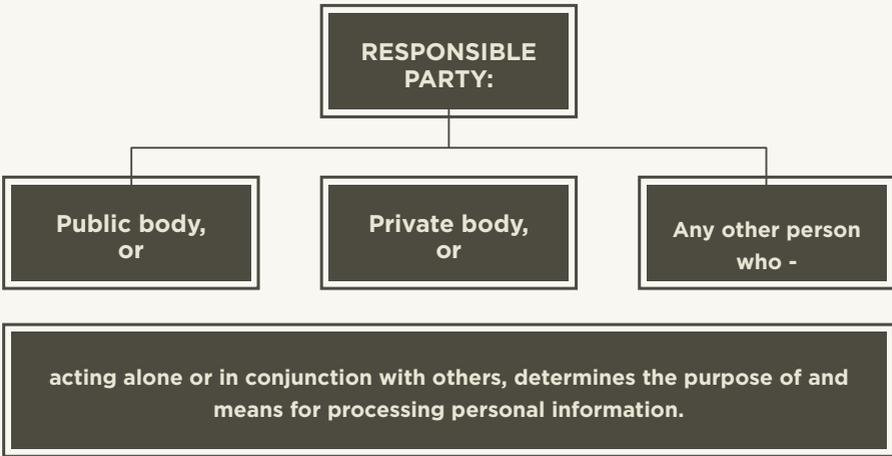


# Chapter 2

## IMPORTANT DEFINITIONS

In order to fully understand the Act and its requirements, it is necessary to first grasp the terms that the Act uses such as responsible party, processing and personal information.

# RESPONSIBLE PARTY



**Figure 1** Definition of responsible party

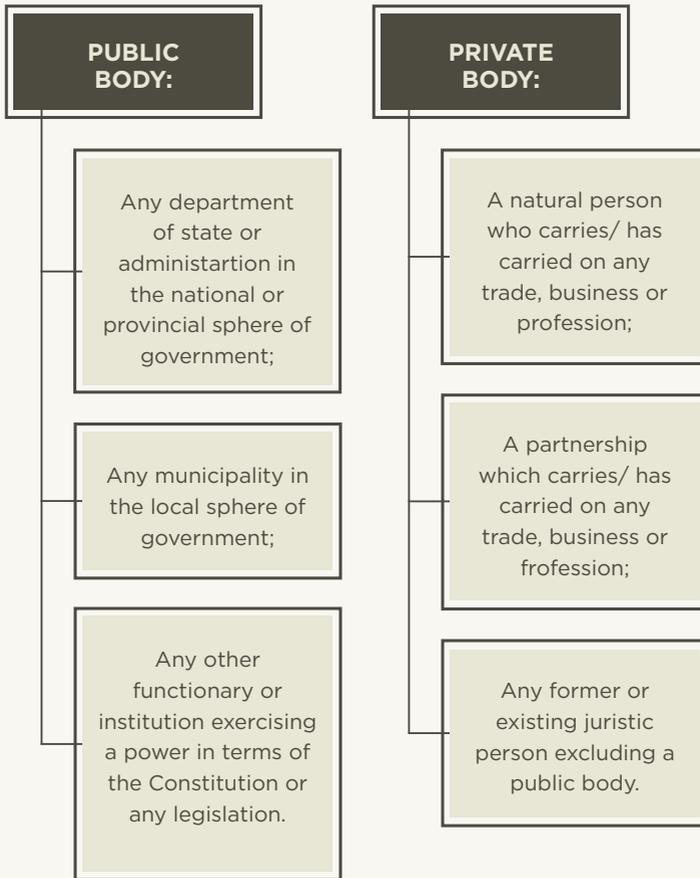
A responsible party can be a public or private body or anyone else who determines the **purpose** of (the reason that the information is needed) and the **means** (how the information will be gathered and processed) for processing personal information. An individual capturing personal information for personal or household activities is not considered a responsible party and is exempt from the Act's requirements.

For example, if a store wanted to launch a loyalty programme, they would need to ask prospective subscribers of the scheme to supply certain personal information. The store would therefore be deemed a responsible party. The purpose of collection would be to create a subscriber profile that would enable the store to record accumulated points and product preferences, communicate with and target promotional material to a loyalty subscriber. The responsible party would then need to determine what personal information is necessary in order to achieve this purpose such as name and surname, identity number, contact details (telephone number and email address) and permission to send communication. The responsible party would have to decide how this information will be collected (means)



which will directly affect how it is processed and captured. For instance, subscribers could be asked to complete a form in-store, call a number or complete an application online. Each one of these options would then have its own challenges for processing.

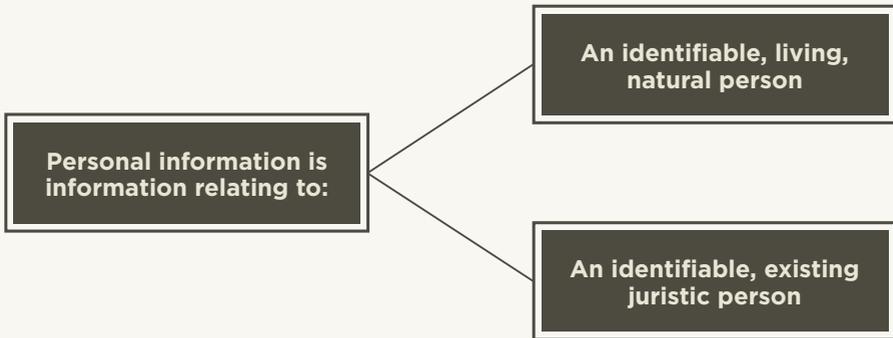
## PUBLIC AND PRIVATE BODIES



**Figure 2** Definition of public and private bodies



Before we look at types of personal information that are covered by the Act, it is important to note that it is not only natural persons' personal information that is covered by the Act but also that of juristic entities (both public and private) such as companies and government departments. In law, a natural person is a human being as opposed to a legal/ juristic person which may be a private or public body.



**Figure 3** Definition of personal information

## TYPES OF PERSONAL INFORMATION

The types of information that are classed as personal information are very broad and include:

- ▶ 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;
- ▶ information relating to the education or the medical, financial, criminal or employment history of the person;
- ▶ any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other



particular assignment to the person such as a Twitter handle or Skype name;

- ▶ the biometric information of the person;
- ▶ the personal opinions, views or preferences of the person;
- ▶ 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;
- ▶ the views or opinions of another individual about the person; and
- ▶ 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;

With regards to the preceding example of the store that wants to establish a [loyalty programme](#), it is clear from the above definition that the majority of the information that the store wants to obtain from the prospective subscriber is in fact personal information. This means that most of the information that they obtain needs to be handled in terms of this Act and must be protected accordingly.

## DATA SUBJECTS

A **data subject** means the person to whom the personal information relates and can be a natural or a juristic person.

A **competent person** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child (a natural person under the age of 18 years).



# DATA SUBJECTS' RIGHTS

Data subjects are granted certain rights under the Act that public and private bodies must uphold. These rights are summarised below and discussed in depth in the chapters that follow.

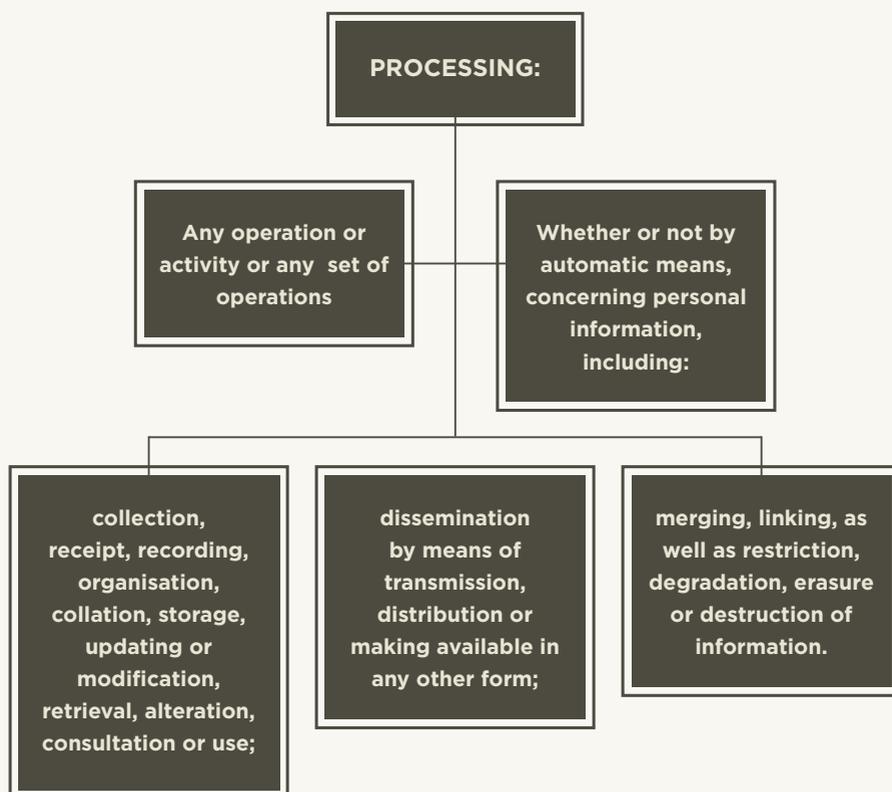
Data subjects have the right to:

- ▶ be notified that information about them is being collected or that their information has already been accessed or acquired by an unauthorised person;
- ▶ establish whether a responsible party holds their personal information and to request access to this personal information;
- ▶ request, where necessary, the correction, destruction or deletion of their personal information;
- ▶ object, on reasonable grounds, the processing of their personal information;
- ▶ object to the processing of personal information for direct marketing purposes;
- ▶ not have their personal information processed for the purposes of direct marketing by means of unwanted electronic communication;
- ▶ not be subject (under certain circumstances) to a decision based solely on the basis of the automated processing of their personal information intended to create a profile of such a person;



- ▶ submit a complaint to the Information Regulator regarding any alleged interference with the protection of any personal information of any data subject;
- ▶ Institute civil proceedings regarding alleged interference with the protection of their personal information.

## DATA PROCESSING



**Figure 4** Definition of processing



From this very broad definition it is clear that virtually any action in relation to personal information would be deemed “processing” and would therefore be subject to the Act unless an [exemption](#) applies. Therefore all public and private bodies will, in some capacity or the other, process personal information in their day-to-day functioning.



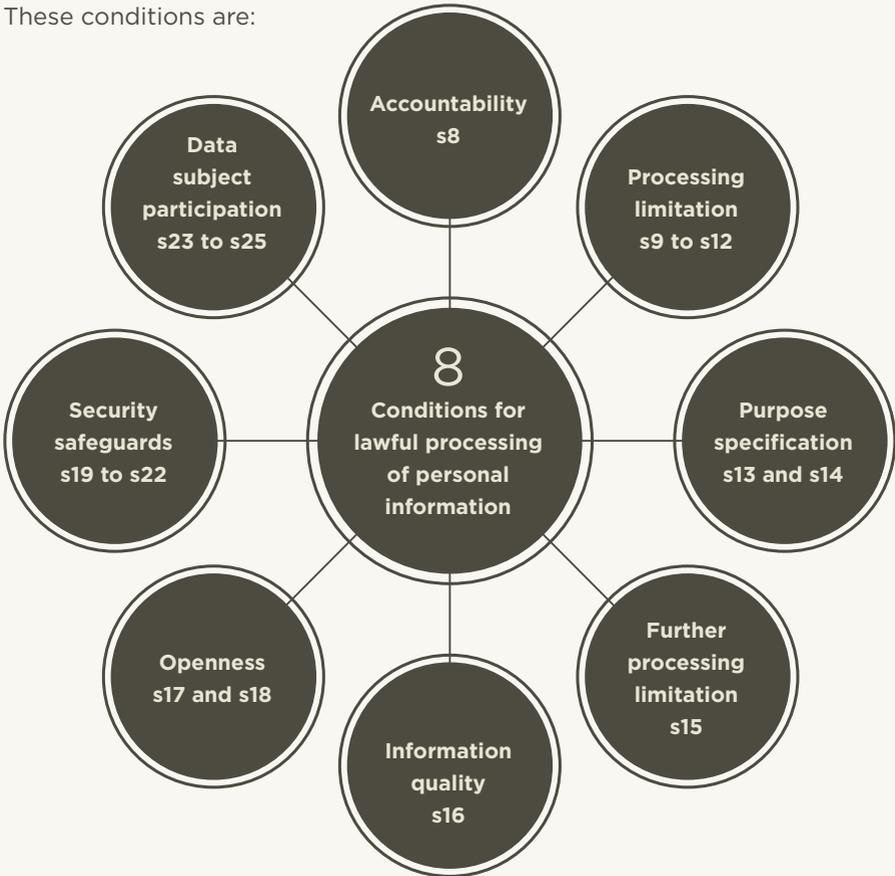


# Chapter 3

## CONDITIONS FOR LAWFUL PROCESSING

The Act sets out eight conditions that must be met in order for the processing of personal information to be legal.

These conditions are:



**Figure 5** Conditions for lawful processing of personal information

## 1. ACCOUNTABILITY

### Section 8

Simply put, this condition states that a responsible party must ensure that all requirements and conditions of the Act are complied with at all times during data collecting, processing and storage as well as when determining the purpose and means of processing the personal information.



## 2. PROCESSING LIMITATION

Sections 9, 10, 11 & 12

Responsible parties must process personal information in a manner that is lawful and does not infringe the privacy of the data subject. An example of unlawful processing would be if the personal information were to be obtained from a third party without the data subject's consent.

Before data is collected, the responsible party must establish the [purpose](#) for which this data is needed. Data may only be processed if it is adequate, relevant and not excessive in relation to its purpose. For example, if the purpose of the data collection was to sign-up customers for a loyalty programme, a responsible party would need to obtain specific information to create a profile for each customer. Just having a name and phone number for the customer would likely not be adequate. Likewise, it would not be relevant for the store to ask for previous work experience or criminal convictions. An example of excessive may be asking for the consumer to fill in a questionnaire about their product preference and use in order to complete the application process.

Personal information may only be processed if:

- ▶ The data subject consents to the processing. Where the data subject is a child, a [competent person](#) must consent on behalf of the child.
- ▶ The data processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party, such as taking out a cellphone contract or filling in a job application form.
- ▶ Processing complies with an obligation imposed by law on the responsible party. For example, when the RICA Act



(The Regulation of Interception of Communication-Related Information Act) was passed, mobile network operators were required by law to register all cellphone numbers on their networks by linking them to an ID number and proof of residence. In such instances a data subject would not be able to object to their personal information being collected and processed.

- ▶ Processing protects a legitimate interest of the data subject
- ▶ Processing is necessary for the proper performance of a public law duty by a public body, for example an arresting police officer would be required to collect personal information from an alleged offender.

It is important to note that the burden of proof for consent falls upon responsible party. Furthermore, this consent may be withdrawn at any time provided that it is legal for the data subject to do so. It is therefore imperative that the responsible party retain, as evidence, any documentation of such consent, as not being able to prove consent could leave them in breach of the Act.

Except where data is being processed in accordance with legislation, a data subject may object at any time to the processing of personal information. This must be done in the prescribed manner and the data subject must have reasonable grounds for their objection. The responsible party would then need to establish if the objection was indeed reasonable. As “reasonable grounds” is such a vague term, it may be necessary to approach the Information Regulator for a ruling in some instances. Once a data subject has objected to the processing, the responsible party may no longer process the personal information. They may only resume processing if the objection is found to be invalid or if they are legally required to do so by law. A data subject may also object to the processing of their personal information for the purposes of direct marketing which will be discussed in further in [Chapter 7](#).



Where a data subject has objected to their information being processed, the responsible party may no longer process the personal information.

Personal information must be collected directly from the data subject (which helps to ensure data accuracy). However there are several exceptions to this:

- ▶ The information is contained in or derived from a public record (such as contact information in a telephone directory) or has been deliberately made public by the data subject (through mediums such as social networks);
- ▶ The data subject has consented to the collection from another source;
- ▶ Collection from another source wouldn't prejudice the legitimate interest of the data subject;
- ▶ Collection from another source is necessary:
  - ▷ To avoid prejudice to the maintenance of the law by any public body that prevents, detects, investigates or prosecutes or punishes offences. For example, members of law enforcement would be allowed to obtain a suspect's details from a third party;
  - ▷ To comply with an obligation imposed by law, such as RICA, or to enforce legislation concerning the collection of revenue – e.g. The South African Revenue Service (SARS) would be able to obtain personal information relating to a data subject's bank accounts directly from the bank;
  - ▷ For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
  - ▷ In the interest of national security – for instance the State Security Agency would be entitled to obtain a data subject's



flight information from Airports Company South Africa without the data subject's consent if they thought that the data subject was involved in any terrorist activity.

- ▷ To maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied.

### 3. PURPOSE SPECIFICATION

Sections 13 & 14

Any personal information that is collected must be done so with a specific, explicitly defined and lawful purpose relating to the function or activity of the responsible party. The data subject must be [made aware](#) of the purpose for which the information is being collected unless certain [exclusions](#) apply.

A responsible party may not retain personal information any longer than is necessary for achieving the purpose for which the information was collected. For example, once an agreement has been concluded, the responsible party is no longer authorised to retain the information. There are, however, some exceptions to this, namely:

- ▶ Retaining the information/ record is required by law;
- ▶ The responsible party requires the record for lawful purposes relating to its functions or activities;
- ▶ Retention of the record is required by contract between the parties;
- ▶ The data subject or competent person has consented to the retention of the record.



Records of personal information may also be kept for extended periods for historical, statistical or research purposes, although the responsible party must ensure that appropriate safeguards are in place against the records being used for any other purpose.

Where a data subject's recorded information has been used to make a decision regarding that data subject, such as a home loan application, the responsible party must retain the record for a period required by law or a code of conduct. Where there is no law or code of conduct, the responsible party is required to retain the record for a period which will afford the data subject a reasonable opportunity to request access to the record. Once again "reasonable opportunity" is a very vague term, with the Act's only guideline being that the use of the personal information should be taken into consideration.

Once a responsible party is no longer authorised to retain the record, they must destroy or delete it, or at least de-identify it as soon as is reasonably practicable. This must be done in a manner that will ensure that it cannot be reconstructed into an understandable form.

To de-identify data means to delete any information that:

- ▶ Identifies the data subject such as a name or ID number;
- ▶ Can be used or manipulated to identify the data subject such as a home address;
- ▶ Can be linked to other information that identifies the data subject

Processing of personal information must be restricted by the responsible party if:

- ▶ The data subject has contested the accuracy;
- ▶ The responsible party has achieved the purpose for which the data was collected/ processed and no longer needs it, but it has to be maintained for the purpose of proof;
- ▶ The processing is unlawful and the data subject has opposed it being deleted or deconstructed or has requested that its use be restricted;
- ▶ The data subject has requested that that the personal information be transmitted into another automated processing system.

Any personal information that is restricted may only be processed:

- ▶ For the purpose of proof;
- ▶ With the data subject or competent person's consent;
- ▶ For the protection of the rights of another natural or legal person; or
- ▶ If such processing is in the public interest.

The responsible party is obligated to notify a data subject of their intention to do so before lifting a processing restriction.



## 4. FURTHER PROCESSING LIMITATION

### Section 15

In order to process personal information further, a responsible party must first establish whether this processing is in accordance with the [purpose](#) for which the data was collected.

To assess purpose compatibility, the responsible party must consider:

- ▶ The purpose of the intended further processing compared to the purpose for which the information was collected;
- ▶ The nature of the information concerned;
- ▶ What consequences, if any, there would be for the data subject;
- ▶ The manner in which the information has been collected;
- ▶ Any contractual rights and obligations between the parties.

Further processing would be deemed to be compatible with the purpose of collection if:

- ▶ The data subject or competent person has consented to further processing;
- ▶ The information is available in or derived from a public record or has been made public deliberately by the data subject.

The Act, however, does provide for some exceptions and allows further processing in the following circumstances:

- ▶ To avoid prejudice to the maintenance of the law;



- ▶ To comply with an obligation imposed by law or enforce legislation concerning collection of revenue;
- ▶ For the conduct of proceedings in any court or tribunal;
- ▶ Where the information is used for historical, statistical or research purposes;
- ▶ Where further processing is in accordance with an [exemption](#) granted under section 37;
- ▶ Where it is in the interest of national security or there is an imminent threat to public health or public safety;
- ▶ Where there is a threat to the life or health of a data subject or another individual.

## 5. INFORMATION QUALITY

### Section 16

It is the duty of the responsible party to take reasonably practicable steps to ensure that personal information is:

- ▶ Complete
- ▶ Accurate
- ▶ Not misleading
- ▶ Updated

This must be done with the purpose for which the personal information was collected in mind.



## 6. OPENNESS

Sections 17 & 18

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act (See [Appendix I](#)).

A responsible party must notify a data subject when collecting their personal information. In this notification, the responsible party must make the data subject aware of:

- ▶ The information being collected as well as the source if it is not being collected from the data subject;
- ▶ The name and address of the responsible party;
- ▶ The purpose for which the information is being collected, such as updating company records or for statistical purposes;
- ▶ Whether or not the supply of info is voluntary or mandatory;
- ▶ Any particular law authorising or requiring the collection of the information such as the RICA Act;
- ▶ The consequences of failure to provide the information, such as cellular service being halted where the data subject did not meet the requirements of RICA;
- ▶ The fact that the responsible party intends to transfer the information to a third country or international organisation as well as what level of protection the information will receive;
- ▶ The recipient or category of recipients of the information;



- ▶ The nature or category of the information;
- ▶ Their right to access or rectify the information collected;
- ▶ Their right to object to their personal information being processed;
- ▶ Their right to lodge a complaint with the Information Regulator.

The data subject must be notified **before** the information is collected, unless the data subject is already aware of all the information that the responsible party is required to disclose. This would be the case where information was previously collected from the data subject (with their knowledge) and subsequent collection is of the same information or information type and the purpose of collection remains the same.

Where information is collected from a third party, the responsible party must still notify the data subject prior to collecting the information, failing which, as soon as reasonably practicable afterwards.

A responsible party would be exempt from adhering to this requirement if to do so would prejudice the maintenance of the law, or if it was in the interest of national security. Non-compliance is also deemed necessary where the information is needed for the conduct of proceedings in any court or concerning the collection of revenue under the SARS Act.

A responsible party would also be able to argue that compliance was not reasonably practicable in certain circumstances or that compliance would prejudice a lawful purpose of the collection.

Information that is used in a form where the data subject is not identifiable or which will be used for historical, statistical or research purposes also need not comply with this condition.



## 7. SECURITY SAFEGUARDS

Sections 19, 20, 21, 22

An organisation that keeps any personal information is responsible for safeguarding that data. Steps must be taken to secure the integrity and the confidentiality of the information and measures need to be put in place to prevent loss of, damage to or unauthorised destruction of personal information. Furthermore, the responsible party must also guard against unlawful access to or processing of personal information. Security safeguards, data breaches and liability will be discussed in more detail in [Chapter 4](#).

## 8. DATA SUBJECT PARTICIPATION

Sections 23, 24 & 25

A data subject has the right to request that a responsible party disclose whether or not they hold any information on the data subject (See [Appendix IV](#)). A responsible party may not charge a fee for such a request although they may demand adequate proof of identity before complying.

The data subject may request the record or a description of what personal information the responsible party holds on them, including information about the identities of all third parties who have or have had access to the information. The responsible party must ensure that this information is provided:

- ▶ Within a reasonable time;
- ▶ At a prescribed fee, if any (while the responsible party may



not charge a fee for confirming or denying that they possess personal information on the data subject, they may impose a fee for providing a copy of the record or a description of the information that is held);

- ▶ In a reasonable manner and format;
- ▶ In a form that is generally understandable.

For example, a data subject may wish to request dental x-rays from a dental practice that they had previously visited. The dental practice would be required to disclose, free of charge, whether or not they are still in possession of the x-rays. Should they still have the x-rays, they would need to tell the data subject what the cost would be to provide a copy of them to the data subject (i.e. a postal fee). The dental practice would need to ensure that this is done in not only a timely manner, but also is in the correct format.

A responsible party that communicates such information to a data subject must advise the data subject that they have a right to request the correction of any information.

For example, a data subject who receives a notice from a credit provider informing them that they are being blacklisted for defaulting on a loan would be entitled to request that the party who sent the notice reveal what personal information they possess on the data subject. The responsible party is required to disclose any third parties that previously or currently have access to that personal information such as any debt collection agency. They would also need to inform the data subject of their right to request that corrections be made.

A responsible party must first give an applicant a written estimate of any fee necessary to enable the responsible party to respond to a request and may require that a deposit be paid.

There are certain grounds on which a responsible party must or may refuse



to disclose requested information. These are listed in Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act (PAIA) and can be found in [Appendix I](#). However, if a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of PAIA, every other part must be disclosed.

Where the personal information requested relates to access to health or other records, sections 30 and 61 of PAIA will apply.

A data subject has the right to request that a responsible party correct or delete personal information about the data subject that is:

- ▶ Inaccurate;
- ▶ Irrelevant;
- ▶ Excessive;
- ▶ Out of date;
- ▶ Incomplete;
- ▶ Misleading;
- ▶ Obtained unlawfully.

If the responsible party is no longer authorised to keep the record, the data subject may request that it be destroyed or deleted.

A responsible party that receives such a request must:

- ▶ Correct the information;
- ▶ Destroy or delete the information;
- ▶ Provide the data subject with credible evidence in support of the information;



- ▶ Attach to the information a note stating that an agreement could not be reached between the responsible party and the data subject and that a correction was requested but was not made.

If the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.

The data subject must be notified by the responsible party of the action taken as a result of the request such as that the data has been successfully corrected or has been deleted as requested.





# Chapter 4

## SECURITY SAFEGUARDS, DATA BREACHES AND LIABILITY

As mentioned in [Chapter 3](#), one of the conditions for lawfully processing personal information is that responsible parties and organisations that keep any personal information are responsible for [safeguarding](#) that data.

In order to adequately meet the requirement for safeguarding information, a responsible party must:

- ▶ Identify all reasonably foreseeable internal and external risks to the personal information in its possession;
- ▶ Establish and maintain appropriate safeguards against identified risks;
- ▶ Regularly verify that the safeguards are effectively implemented;
- ▶ Ensure that the safeguards are continuously updated.

If, for example, a company had identified fire as a possible risk to the safety of their personal data, they would need to ensure that appropriate measures had been taken such as installing a fire suppression system and ensuring regular back-ups to an off-site facility. Similarly a company could implement a fingerprint or retina scanner requirement to access personal financial information to ensure that only authorised employees have access. A responsible party should also take information security practices in their specific industry into consideration. As technology changes and new threats emerge, so too must a company's data safeguards evolve and grow.

## CYBER-CRIME

Cyber-crime refers to any illegal activities utilising, or against, computer systems or networks, and the internet including criminal acts such as hacking, phishing, and denial or service attacks.<sup>5</sup>

---

5 Ganatra, A., Kosta, Y., Patel, M. & Patel, N. (2008). E-commerce and Attached E-Risk with Cyber-crime. Chang: Computer / Information Technology Department, Charotar University of Science and Technology



Forms of cyber-crime include:

**Denial of Service (DOS) Attack** - a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.<sup>6</sup>

**Malicious Software (Malware)** - software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.<sup>7</sup> This malicious software can enable cyber-criminals to invade a computer undetected, take control of it and extract sensitive documents.

**Industrial (Cyber) Espionage** - the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.<sup>8</sup>

**Phishing** - the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.<sup>9</sup>

South Africa is particularly prone to phishing schemes and is the second most targeted country globally according to information security and privacy practice 4Di Privaca.<sup>10</sup>

With a phishing scheme, unsuspecting victims are sent emails falsely

---

6 [www.incapsula.com/ddos/ddos-attacks/denial-of-service.html](http://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html)

7 [www.webopedia.com/TERM/M/malware.html](http://www.webopedia.com/TERM/M/malware.html)

8 [http://en.wikipedia.org/wiki/Cyber\\_spying](http://en.wikipedia.org/wiki/Cyber_spying)

9 <http://en.wikipedia.org/wiki/Phishing>

10 <http://www.itnewsafrika.com/2014/04/south-africa-is-second-most-targeted-for-phishing-attacks/>



claiming to be from an established organisation. These emails are sent in an attempt to solicit personal information such as bank account details. The emails often contain a link to a fraudulent website where users are asked to update their personal information. Cyber-criminals then use this personal information to obtain funds or sell the data on to clearing houses.

The South African Revenue Service (SARS) has been a favoured front for cyber-criminals trying to obtain personal information. Over the last five years SARS has issued more than 50 warnings to consumers about scams being perpetuated under their name.

The SARS website contains the following stringent warning:

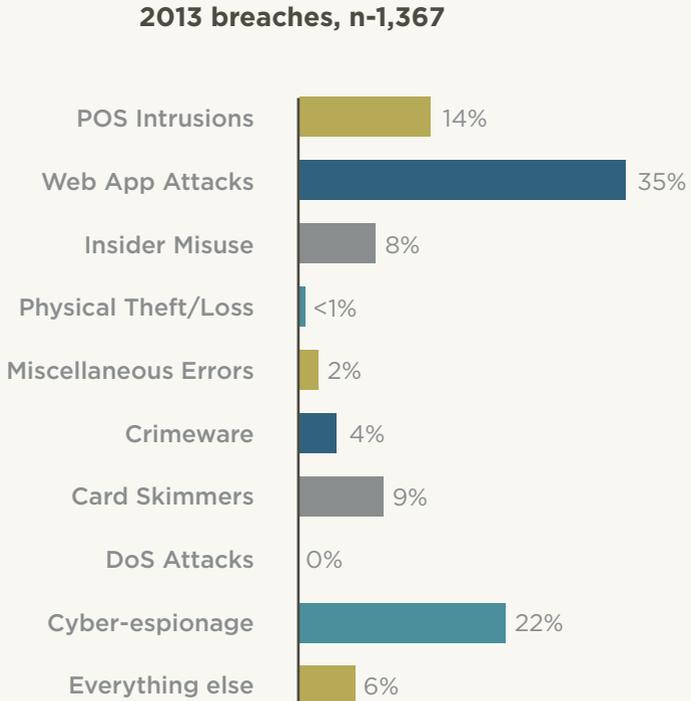
**Members of the public are randomly emailed with false “spoofed” emails made to look as if these emails were sent from SARS, but are in fact fraudulent emails aimed at enticing unsuspecting taxpayers to part with personal information such as bank account details. Examples include emails that appear to be from [returns@sars.co.za](mailto:returns@sars.co.za) or [refunds@sars.co.za](mailto:refunds@sars.co.za) indicating that tax payers are eligible to receive TAX refunds. These emails contain links to false forms and false websites made to look like the “real thing”, but with the aim of fooling people into entering personal information such as bank account details which the criminals then extract and use fraudulently.**

SARS has dedicated a section of their website to educating and informing consumers about the various scams that have been doing the rounds which can be accessed at <http://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx>. In [Appendix II](#) you will find some examples of these SARS phishing scams.



# TYPES OF DATA BREACHES

Verizon, an American organisation that specialises in communications and technology, releases an annual Data Breach Investigation Report which it compiles with the help fifty international organisations ranging from security companies and audit firms, to authorities such as the United States Department of Homeland Security. According to the 2013 report, web application attacks - which would include phishing scams - were the most frequently occurring form of cyber-attack at 35%. Next was Cyber Espionage at 22% and Point of Sales Intrusions which account for 14% of reported incidents.



**Figure 6** Frequency of incident classification patterns (Verizon Enterprise Solutions, 2013)



The following list<sup>11</sup> serves to demonstrate just how at risk of data breaches companies have become as a result of hacking<sup>12</sup> in recent years and on what a massive scale they can occur.

- ▶ Epsilon, the world's largest provider of permission-based email marketing, revealed in March 2011 that they had been hacked. The hack exposed the names and email addresses of tens of millions of customers.
- ▶ The April 2011 cyber-attack on electronics giant Sony's Playstation Network (PSN) affected more than 77 million users. The company warned that names, addresses, birthdates, PSN passwords and credit card numbers may have been acquired.
- ▶ Credit card processor service Global Payment Systems discovered in March 2012 that 1.5 million credit card records had been stolen and a further 5.5 million consumer records. In January 2013 the company revealed that the breach had cost them more than \$93.9 million.
- ▶ In January 2012 online shoe and clothing retailer Zappos notified customers to a breach that had potentially exposed the names, addresses (billing and shipping), phone numbers and partial credit card numbers (the last four digits) of their 24 million users to the hackers.
- ▶ The account information of about 38 million Adobe users was exposed in a data breach in October 2013. Adobe revealed that encrypted customer credit card records were stolen as

---

11 List adapted from <http://m.golocalprov.com/news/10-big-companies-with-recent-major-security-breaches/> (accessed 3 July 2014)

12 Oxford Dictionaries defines hacking as: (To) Gain unauthorized access to data in a system or computer (<http://www.oxforddictionaries.com/definition/english/hack?q=hacking>)



well as login data for an undetermined number of Adobe user accounts.

- ▶ Target's CEO Gregg Steinhafle tendered his resignation in December 2013 after the company announced that 110 million customers' personal information had been breached. More than 40 million customers had their encrypted pin numbers, credit card and debit card numbers, card expiration dates, as well as the embedded code on the magnetic strip stolen. A further 70 million customers' personal information which included names, addresses, email addresses and phone numbers were also compromised.
- ▶ Despite nearly 60 000 security alerts being set off in the four month period between July and October 2013, luxury department Neiman Marcus only discovered the data breaches in January 2014. The retailer was in compliance with standards meant to protect transaction data when the attack occurred. 350 000 customers' credit card information was stolen and of these 9200 have been used fraudulently since the attack [as of May 2014].
- ▶ Up to 145 million eBay customers have potentially had their personal information leaked the company admitted in May 2014. While email addresses, phone numbers and other details were hacked, eBay insist that there is no evidence that financial data was compromised.

## eBay's data breach examined

eBay has been fiercely criticised for the manner in which they handled a recent data breach that exposed an estimated 145 million users' personal information. Not only did the breach go undetected for nearly three



months, but eBay took a further two weeks to make an announcement. The [announcement](#), which did not appear on [eBay.com](#) but rather on the seldom viewed corporate website [Ebayinc.com](#), warned customers that a cyberattack had occurred which compromised a database containing names, phone numbers, home addresses, emails and encrypted passwords but not financial information.

The company made matters worse by not immediately notifying customers of the breach via email. Instead, many users were only made aware of the attack through media reports. The company has since put a request on [eBay.com](#) for users to change their passwords as well as a link to the announcement. Furthermore, many industry experts have lamented the fact the password change is optional and not enforced.

Under the Protection of Personal Information Act, a responsible party may only delay notifying affected data subjects if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to the data subject must be in writing and must be communicated in at least one of the following ways:

- ▶ Mailed to the data subject's last known physical or postal address;
- ▶ Sent by email to data subject's last known address;
- ▶ Placed on a prominent position on the website of the responsible party;
- ▶ Published in the news media;
- ▶ As may be directed by the Regulator.



Further, this notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the security compromise, including:

- ▶ A description of the possible consequences of the security breach (e.g. that you may become the victim of identity theft or that your credit card information was exposed leaving you vulnerable financially);
- ▶ A description of the measures that the responsible party intends to take or has taken to address the security compromise (such as all user accounts have been frozen until security has been upgraded);
- ▶ A recommendation with regards to the measures to be taken by the data subject to prevent negative consequences of the breach (change site password or cancel credit card);
- ▶ The identity of the unauthorised person, if known, who may have accessed or acquired the personal information (such as a hacking group that has taken credit for the attack).

While some experts have called eBay's handling of their data breach more embarrassing than the breach itself, the company did do itself a service by ensuring that their notification was thorough.

[Appendix III](#) includes a screen capture of the warning that appeared on eBay's website with a link to the announcement concerning the security breach.

Under POPI, the Regulator may demand that a responsible party publicise (in a specified manner) the fact that personal information has been compromised where there are grounds to believe that such publicity would protect the data subject who may be affected by the compromise.



# IDENTITY THEFT

Identity theft refers to personal information which has been obtained fraudulently through phishing scams, malware, and spyware or by other means. This information can be used by cyber-criminals to commit fraud or are sold on to other criminals.

## Dangers of data breaches to consumers

According to [www.CIO.com](http://www.CIO.com),<sup>13</sup> a company that delivers the latest tech news and analysis, personal information is the currency of the underground economy and is what cybercriminals trade in. Hackers that have obtained personal information are able to sell this data to a variety of different buyers such as identity thieves, organised crime rings, spammers and botnet operators.

All a cybercriminal needs is an email address to start doing damage. The most common security risk for consumers who have had their personal information exposed is an increase in spam emails. However, these may include targeted phishing<sup>14</sup> emails which are dangerous as they attempt to trick the recipient into clicking a link that will download malicious malware (that installs key-logging software that can record usernames and passwords) or will attempt to solicit confidential information like passwords or credit card information.

---

13 <http://www.cio.com/article/2400064/security0/are-you-at-risk--what-cybercriminals-do-with-your-personal-data.html>

14 Oxford Dictionaries defines phishing as: The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online (<http://www.oxforddictionaries.com/definition/english/phishing>)



The more personal information a cybercriminal can obtain on a victim, the more convincing and effective the phishing schemes can be. Some cybercriminals will even send out a fake breach disclosure notification advising victims to reset their passwords on a website that looks real but is fake.

With regard to financial information, the last 4 digits of a credit or debit card may be enough to reset your password on an ecommerce site – enabling cybercriminals to make purchases using your account. Where cybercriminals obtain complete credit card numbers they will likely start using this information immediately.

## Operators

The Act defines an operator as 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. For instance, someone working in a call centre that has been outsourced by an insurance firm would be deemed to be an operator even though they are employed by the call centre and not the insurer.

The Act imposes certain obligations on these operators such as that they may not process personal information without the knowledge and authorisation of the responsible party. Operators are also required to treat all information which comes to their attention as confidential and may not disclose it unless required by law or in the course of the proper performance of their duties.

A written agreement must be in place between the responsible party and the operator to ensure that the operator maintains the security measures that are in place to protect the data. The operator has a duty to notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person. Should a breach have occurred, the



responsible party must notify the Information Regulator. The affected data subject/s must also be notified unless their identity cannot be established. This notification must happen as soon as possible after discovery of the compromise. However, the responsible party may first determine the scope of the compromise and restore the integrity of the of the information system before notifying the affected data subjects.

**Outsourcing data collection and/or data storage does not mean that the liability is also outsourced. You are responsible even if the breach is as a result of operator fault.**

## POTENTIAL LIABILITY UNDER POPI

There are three elements of potential liability stemming from the Act that organisations and operators would should be aware of:

1. Civil liability for patrimonial (relating to direct financial loss such as medical expenses) and non-patrimonial damages (damages that cannot be related to a person's financial estate, but compensation for something like pain and suffering) for interference with personal information (whether or not there is intent or negligence);
2. Criminal liability not exceeding ten years and / or the payment of a fine; and
3. Administrative liability for an [administrative penalty](#) payable to the Information Regulator, to the maximum of R10 million.

[Civil liability](#) gives a person the right to obtain redress from another person i.e. the ability to sue for damages for personal injury or loss. Where a data subject's personal information has been compromised as a result of



a responsible party's data breach and the data subject has suffered from financial loss or even pain and suffering, the data subject would be able to sue the responsible party to recoup these losses. The fact that data subjects can now hold responsible parties liable for breaches to their personal data will have huge financial ramifications on organisations that store personal information.

Penalties, enforcement and civil liability are discussed further in [Chapter 8](#).

## CYBER LIABILITY INSURANCE

While it is true that prevention is better than cure, it is strongly advisable that responsible parties have adequate cyber liability insurance in place. Even with a combination of technology and security procedures in position, it is not always possible to ensure complete protection, especially given the fact that cyber attackers are continuously seeking new methods to exploit vulnerabilities.<sup>15</sup>

Almost every company has some kind of network, database or online presence that puts it at risk. The complexity of the online environment makes it impossible for most businesses to address these risks, or even appreciate how serious the threat is.

The effect of a cyber-attack could be devastating to almost any business: network down-time, loss of important data and loss of credibility when customer information is compromised (not to mention the litigation that would follow if the hacker were to use that information to plunder the customer's bank account).

---

15 Jain, A. & Kalyanam, S. (2012). *Using insurance to mitigate cybercrime risk: challenges and recommendations for insurers*. [https://www.capgemini.com/resource-file-access/resource/pdf/Using\\_Insurance\\_to\\_Mitigate\\_Cybercrime\\_Risk.pdf](https://www.capgemini.com/resource-file-access/resource/pdf/Using_Insurance_to_Mitigate_Cybercrime_Risk.pdf)



The South African cyber insurance market is growing quickly in response to an increasing demand for cyber cover. To meet this demand, Camargue, a specialist liability underwriting agency, has introduced a cyber insurance policy aimed at protecting South African businesses from the devastating effects of a cyber attack.

## CAMARGUE'S CYBER LIABILITY COVER

Camargue's e-risks policy covers organisations against the risks arising out of operating a computer network. In addition to this,

- ▶ It covers liability arising from online publishing (such as a web site) as well as from traditional media (such as brochures);
- ▶ There is an option which provides professional indemnity cover appropriate to companies which participate in developing software and other technology;
- ▶ It not only covers the Insured's liabilities to others, it also provides a form of specialised business interruption cover which covers the Insured's loss of income arising out of computer down-time.

In addition to these, the policy also covers:

- ▶ Technology & miscellaneous E&O
- ▶ Multimedia liability
- ▶ Security & privacy liability
- ▶ Data recovery & loss of business income



- ▶ Privacy regulatory defence & penalties
- ▶ Crisis management costs, including customer notification, support and credit monitoring expenses
- ▶ Data extortion

Notwithstanding the coverage provided in terms of the policy, the additional risk management benefits further enhance the Camargue product offering and go beyond simple insurance. The overall result is a well-rounded and complete solution to the risks faced by businesses.





# Chapter 5

## PROCESSING OF SPECIAL PERSONAL INFORMATION

There are certain types of information, called special personal information by the Act, that a responsible party is prohibited from processing.

These include:

- ▶ Religious or philosophical beliefs;
- ▶ Race or ethnic origin;
- ▶ Trade union membership;
- ▶ Political persuasion;
- ▶ Health or sex life;
- ▶ Biometric information.

A responsible party may also not process information relating to the criminal behaviour of a data subject such as an alleged commission of any offence or any proceedings in respect of an alleged offence.

## GENERAL AUTHORISATION

There are, however, some exemptions to this prohibition. For instance, a data subject may consent to the processing of their special personal information or such information has willingly been made public by the data subject. This information can also be processed for the establishment, exercise or defence of a right or obligation in law or to comply with an obligation of international public law.

Where processing is for historical, statistical or research purposes, the responsible party may forego authorisation if the purpose of the processing serves a public interest and the processing will not adversely affect the individual privacy of the data subject to a disproportionate extent.



The Regulator may authorise a responsible party to process special personal information where such processing is in the public interest and appropriate safeguards have been put in place.

## PRIOR AUTHORISATION

In certain circumstances, the responsible party is required to obtain authorisation from the Regulator **prior** to any processing that the responsible party plans to undertake.

Prior authorisation is required to:

- ▶ Process any unique identifiers:
  - ▷ For a purpose other than the one for which the identifier was specifically intended or collected;
  - ▷ With the aim of linking the information with information processed by other responsible parties;
- ▶ Process information on criminal behaviour or unlawful or objectionable conduct on behalf of third parties;
- ▶ Process information for the purpose of credit reporting;
- ▶ Transfer special personal information or personal information of children to a third party in a foreign country that does not provide an adequate level of protection for its processing.

A responsible party may only begin processing this information once the Regulator has notified them that an investigation has been completed or that a more detailed investigation will not take place. The Regulator must



put this in writing to the responsible party within **four weeks** of receiving a request for authorisation. Should a detailed investigation be necessary, this must be completed by the Regulator in a period not exceeding 13 weeks.

## EXEMPTIONS

### Authorisation concerning a data subject's religious or philosophical beliefs

#### Section 28

Spiritual and religious organisations (or independent sections of those organisations) may process a data subject's religious or philosophical beliefs only if the data subject belongs to the organisation and it is necessary to achieve their aims and principles. This exemption also allows the organisation to process the personal religious or philosophical beliefs of family members of the data subject – so long as they have not objected in writing and are in regular contact with the association. The organisation may also process the special information of their employees and any other person belonging to the organisation.

A data subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

### Authorisation concerning data subject's race or ethnic origin

#### Section 29

A responsible party may not process a data subject's personal information regarding their race or ethnic origin unless it is for the purpose of identifying



the data subject. It is also permissible to process this information when complying with the law and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

For example, a recruitment company would be permitted to ask candidates to disclose their race or ethnic origin as these criteria would be used to source suitable candidates to fulfil the requirements of the Broad-Based Black Economic Empowerment Act. However, an organisation such as a marketing firm or a hotel would not legally be able to collect or process this information.

## **Authorisation concerning a data subject's trade union membership**

### Section 30

Trade unions are exempt from the prohibition on processing a data subject's trade union membership information so long as the data subject belongs to that trade union. The trade union federation, to which the trade union belongs, may also process this information. Information relating to trade union membership may not be supplied to any third parties unless the data subject has given consent.

## **Authorisation concerning a data subject's political persuasion**

### Section 31

The restriction on processing a data subject's political persuasion does not apply to institutions founded on political principles when the personal information is for members or employees of the institution. This information may also be processed for the purpose of forming a political



party or participating in the activities of a political party such as canvassing supporters or campaigning.

## Authorisation concerning a data subject's health or sex life

### Section 32

Medical professionals, healthcare institutions and facilities and social services may process information relating to a data subject's health or sex life where such information is necessary for the proper care and treatment of the data subject or the administration of the institution.

Insurance companies, medical aid schemes and their administrators as well as managed healthcare organisations may process this type of information to:

- ▶ Assess the risk to be insured (by the insurance company) or to be covered (by the medical aid scheme) and the data subject has not objected;
- ▶ Perform an insurance or medical aid agreement;
- ▶ Enforce any contractual rights and obligations.

Schools may only process such information when it is necessary to provide special support for pupils or for making special arrangements in connection with their health or sex life. A public or private body who manages the care of a child may only process this information if it is necessary for the performance of their legal duties.

A public body may also process this type of information in connection of the implementation of a prison sentence or detention measures.



Administrative bodies, pension funds, employers or institutions working for them, are also exempt from this restriction if such processing is necessary for the:

- ▶ Implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
- ▶ Reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

All these exemptions are granted on the basis that the information may only be processed by responsible parties subject to an **obligation of confidentiality**. This confidentiality can either be by virtue of office, employment, profession, legal provision or established by a written agreement.

A responsible party that is not subject to an obligation of confidentiality must still treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information.

This prohibition does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health with a view to the proper treatment or care of the data subject.

Any personal information concerning the inherited characteristics of a data subject may not be processed unless:

- ▶ A serious medical interest prevails; or
- ▶ The processing is necessary for historical, statistical or research activity.



## Authorisation concerning a data subject's criminal behaviour or biometric information

### Section 33

Bodies, such as the police, that are charged by law with applying criminal law may process a data subject's criminal behaviour or biometric information.

**Biometrics means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.**

A responsible party may only process such information if it has been obtained in accordance with the law. Where a responsible party processes this information with regard to the personnel in their service, they need to do so in accordance with labour legislation.



# Chapter 6

## PROCESSING OF PERSONAL INFORMATION OF CHILDREN

In general, a responsible party may not process personal information concerning a child.

There are some exceptions to this prohibition. Processing of a child's personal information may be carried out:

- ▶ With the consent of a competent person;
- ▶ Where it is necessary for the establishment, exercise or defence of a right or obligation in law;
- ▶ Where it is necessary to comply with an obligation of international public law;
- ▶ The personal information has deliberately been made public by the child with the consent of a competent person;
- ▶ For historical, statistical or research purposes to the extent that the purpose serves a [public interest](#) or it would be virtually impossible to ask for consent. There must be sufficient guarantees in place to ensure that the processing doesn't negatively affect the privacy of the child.

The Regulator may authorise a responsible party to process the personal information of children if processing is in the public interest and appropriate safeguards are in place. This authorisation may come with certain conditions imposed.





# Chapter 7

## DIRECT MARKETING, DIRECTORIES AND AUTOMATED DECISION MAKING

### **DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATIONS**

The Consumer Protection Act, which came into effect in 2011, already gives consumers various rights regarding direct marketing.

These include the right to restrict unwanted direct marketing, the right to a cooling-off period after direct marketing as well regulated times for contacting a consumer. Chapter 8 of The Protection of Personal Information Act further strengthens these rights by ensuring that a responsible party has obtained consent before contacting a data subject.

Direct marketing is defined as approaching a data subject either in person or by mail or electronic communication (via telephone, fax, sms, email etc.) with the purpose of **promoting** or **offering to supply** goods or services to the data subject or requesting that the data subject make a **donation** of any kind.

Direct marketing communication has been a topic of much debate since the Consumer Protection Act's implementation. The National Consumer Commission were tasked, under section 11 of the Act, with establishing a register where consumers who did not wish to receive unwanted marketing communication could submit their details and pre-emptively block such communication. However, more than four years down the line no such register has been established and "spam" remains a problem.

Section 69 of POPI adds further challenges for direct marketers as it requires that a data subject must give consent before a responsible party can process their information for the purpose of direct marketing. Where a data subject is already a customer of a responsible party, the party may contact the data subject with direct marketing if:

- ▶ The data subject's contact details were obtained through a sale of a product or service;
- ▶ The communication is to market the responsible party's own similar products or services;
- ▶ The data subject has been given opportunity to object to the use of their details when the information was collected and on subsequent communication with the data subject.



The most common way for a data subject to give consent would be by ticking a box on an application form or online stating that they can be contacted. The burden of proof will lie on the responsible party so it is important that records of consent are kept in case any disputes arise.

A responsible party may approach a data subject to obtain consent. However, this may only happen **once**. If the data subject has previously refused consent, the responsible party may not contact them again for the purpose of direct marketing.

## DIRECTORIES

Printed or electronic directories of subscribers that are available to the public such as telephone directories or their electronic counterparts are also governed under this Act. Where a data subject's personal information is included in such a directory, the data subject must be informed free of charge and before the information is included into the directory. The data subject must also be made aware of the purpose of the directory as well as possible further uses based on search functions embedded in electronic versions.

For example, an organisation such as a church may wish to put together a directory of all their members so that their details are readily available to other members. Before doing so, the church must first notify each member whose details will appear in the directory to inform them of the directory as well as its purpose. If the church plans to host an electronic version of the directory on their website that links member details to a member profile then this would also need to be disclosed.

A data subject should be able to object, in an informal manner, to their personal information being used. Likewise, they should be given the



opportunity to verify, confirm or withdraw their personal information. This does not apply to editions of directories (both print and electronic) that were produced before the commencement of section 70 of the Act.

## AUTOMATED DECISION MAKING

Automated decision making has become possible with the evolution of technology. While it is still a relatively new process in South Africa, the Act has taken the foresightful step of regulating its use.

Under Section 71, responsible parties may not subject data subjects to automated decisions that will result in legal consequences or will harm them to a substantial degree if the decision is solely based on the automated processing of personal information intended to provide a profile of such a person. This includes information pertaining to work performance, credit worthiness, reliability, location, health, personal preferences or conduct.

However this does not apply if the decision has been taken in connection with the conclusion or exclusion of a contract and the request of the data subject has been met or appropriate measures have been taken to protect the data subject's legitimate interests.

The appropriate measures mentioned include providing:

- ▶ An opportunity for a data subject to make representations about a decision;
- ▶ A data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations.



While not common in South Africa, there are some companies such as [Wonga.com](https://www.wonga.co.za) that already use automated decision making.

[Wonga.com](https://www.wonga.co.za) is a short-term loans provider that relies automated decision-making to approve small cash loans. According to their CEO in South Africa, Kevin Hurwitz, their service uses patented technology which accesses thousands of points of publicly-available data in order to make an instant yet accurate lending decision. “We believe that because we make our lending decisions without the need for human intervention or hard documentation, our decisions are more likely to be accurate as there is no room for subjectivity or human bias” says Hurwitz.<sup>16</sup>

Under the Act, if a data subject were to be rejected for a [Wonga.com](https://www.wonga.co.za) loan and this decision was an automated one, the data subject would be able to query this decision. The responsible party, in this case Wonga, would then need to inform the data subject on what basis their application was rejected. For example, the automated system may have detected that the data subject has a bad credit record which could be perceived as affecting their ability to repay the loan.

---

<sup>16</sup> <https://www.wonga.co.za/blog/wongacom-brings-its-automated-loans-service-south-africa>





# Chapter 8

## PENALTIES AND ENFORCEMENT

### INFORMATION REGULATOR

The Act would be meaningless if there were no body to enforce it. In order to ensure the Act's success, Section 39 establishes the juristic position of Information Regulator who will have jurisdiction throughout the republic.

The Regulator's duties will include:

- ▶ **Educating** data subjects through educational programmes;
- ▶ **Monitoring** and enforcing compliance by public and private bodies;
- ▶ **Consulting** with interested parties;
- ▶ Handling and investigating **complaints** about alleged violations;
- ▶ Conducting research;
- ▶ Issue, amend or revoke **codes of conduct**;
- ▶ **Facilitate** cross-border **cooperation** in the enforcement of privacy laws.

The section of the Act that deals with the establishment and duties of the Information Regulator (Chapter 5, Part A) came into effect on 11 April 2014 along with several other [sections](#).

## COMPLAINTS

Any person who feels that their rights as a data subject have been infringed may submit a complaint to the Regulator in writing. Likewise, a responsible party may also approach the Regulator if they are aggrieved by the decision of an adjudicator.



# PENALTIES

Any person convicted of an offence, in terms of the Act, is liable to a [fine](#) of up to **R10 million** or imprisonment depending on the offence. Prison sentences vary and are under **12 months** for lesser offences and up to **ten years** for gross offences.

# OFFENCES

Chapter 11 lists punishable offences under the Act which are in addition to the offence of failing to comply with the conditions for lawful processing. The Magistrate’s Court has jurisdiction to impose any penalty provided for in the table below.

These offences are:

Offence	Section	Penalty
<a href="#">Failure to notify processing subject prior to authorisation</a>	Section 59	A <b>fine</b> or imprisonment not exceeding <b>12 months</b> or both
Breach of confidentiality	Section 101	
Obstruction of execution warrant	Section 102	
Failure to comply with enforcement or information notices;	Section 103 (1)	
Offences by witnesses (such as failing to attend to give evidence or failing to produce evidence in their possession)	Section 104(1)	



Offence	Section	Penalty
Obstruction of the Regulator	Section 100	A <b>fine</b> or imprisonment not exceeding <b>10 years</b> or both
Failure to comply with enforcement or information notices	Section 103 (1)	
Offences by witnesses (giving false evidence)	Section 104 (2)	
Unlawful acts by responsible party in connection with an account number	Section 105 (1)	
Unlawful acts by third parties in connection with an account number	Section 106 (1) (3) or (4)	

## ADMINISTRATIVE FINES

Where a responsible party is alleged to have committed an offence in terms of this Act, the Regulator may issue an infringement notice. This notice must include the amount of the administrative fine that is payable by the responsible party (if any).

The Regulator must consider the following factors when determining an appropriate fine:

- ▶ The nature of the personal information involved;
- ▶ The duration and extent of the contravention;
- ▶ Number of data subjects affected or potentially affected (by the contravention);
- ▶ Whether or not the contravention raises an issue of public importance;



- ▶ The likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;
- ▶ Whether the responsible party or a third party could have prevented the contravention;
- ▶ Failure to carry out risk assessment or failure to operate good policies, procedures and practices (to protect personal information);
- ▶ Whether the responsible party has previously committed an offence in terms of this Act.

The infringement notice must also inform the infringer that they have 30 days in which to pay the administrative fine, make arrangements with the Regulator to pay the fine in instalments or elect to be tried in court.

If an infringer elects to be tried in court on a charge of having committed the alleged offence in terms of this Act, the Regulator must hand the matter over to the South African Police Service and inform the infringer accordingly.

## **CIVIL ACTION FOR DAMAGES**

Where a data breach has occurred (regardless of whether or not there was intent or negligence on the part of the responsible party), an affected data subject has the right to institute a civil action (in a court having jurisdiction) for damages against the responsible party (i.e. they may sue the responsible party). This may be done by the Regulator on behalf of the data subject or by the data subject themselves.



A responsible party, in turn, may raise the following defences:

- ▶ *Vis major*<sup>17</sup>;
- ▶ Consent of the plaintiff;
- ▶ Fault on the part of the plaintiff;
- ▶ Compliance was not reasonably practicable in the circumstances;
- ▶ The regulator has granted an [exemption](#).

The court hearing the proceedings may award an amount that includes:

- ▶ Payment of damages as compensation for patrimonial (a reduction in a person's financial position, such as is the case where the claimant incurred medical expenses) and non-patrimonial (damages that cannot be related to a person's financial estate, but compensation for something like pain and suffering) loss suffered by a data subject as a result of breach of the provisions of this Act;
- ▶ Aggravated damages, in a sum determined in the discretion of the Court;
- ▶ Interest; and
- ▶ Costs of suit on such scale as may be determined by the Court.

Any civil action instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court.

---

<sup>17</sup> A Latin term meaning “act of God”, or an occurrence that is neither caused by nor preventable by humans. In commercial contracts, *vis major* can also apply to actions undertaken by third parties that neither party to the contract can control, such as failure by a supplier or subcontractor to perform. The terms “*vis major*”, “act of God” and “*force majeure*” are commonly used in contracts to exclude one or both parties from liability and/or obligation when events beyond their control occur (<http://www.investopedia.com/terms/v/vis-major.asp>)





# Appendix

## Extract of Sections 14 and 51 of the Promotion of Access to Information Act.

### 14 Manual on functions of, and index of records held by, **public body**

(1) Within six months after the commencement of this section or the coming into existence of a public body, the information officer of the public body concerned must compile in at least three official languages a manual containing-

(a) a description of its structure and functions;

(b) the postal and street address, phone and fax number and, if available, electronic mail address of the information officer of the body and of every deputy information officer of the body appointed in terms of section 17 (1);

(c) a description of the guide referred to in section 10, if available, and how to obtain access to it;

(d) sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject;

(e) the latest notice, in terms of section 15 (2), if any, regarding the categories of records of the body which are available without a person having to request access in terms of this Act;

(f) a description of the services available to members of the public from the body and how to gain access to those services;

(g) a description of any arrangement or provision for a person (other than a public body referred to in paragraph (a) or (b) (i) of the definition of 'public body' in section 1) by consultation, making representations or otherwise, to participate in or influence-

(i) the formulation of policy; or

(ii) the exercise of powers or performance of duties, by the body;

(h) a description of all remedies available in respect of an act or a failure to act by the body; and

(i) such other information as may be prescribed.

(2) A public body must, if necessary, update and publish its manual referred to in subsection (1) at intervals of not more than one year.

(3) Each manual must be made available as prescribed.

(4) (a) If the functions of two or more public bodies are closely connected, the Minister may on request or of his or her own accord determine that the two or more bodies compile one manual only.



(b) The public bodies in question must share the cost of the compilation and making available of such manual as the Minister determines.

(5) For security, administrative or financial reasons, the Minister may, on request or of his or her own accord by notice in the Gazette, exempt any public body or category of public bodies from any provision of this section for such period as the Minister thinks fit,

#### 51 Manual (private body)

(1) Within six months after the commencement of this section or the coming into existence of the private body concerned the head of a private body must compile a manual containing-

(a) the postal and street address, phone and fax number and, if available, electronic mail address of the head of the body;

(b) a description of the guide referred to in section 10, if available, and how to obtain access to it;

(c) the latest notice in terms of section 52 (2), if any, regarding the categories of record of the body which are available without a person having to request access in terms of this Act;

(d) a description of the records of the body which are available in accordance with any other legislation;

(e) sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject; and

(f) such other information as may be prescribed.

(2) The head of a private body must on a regular basis update the manual referred to in subsection (1).



(3) Each manual must be made available as prescribed.

(4) For security, administrative or financial reasons, the Minister may, on request or of his or her own accord by notice in the Gazette, exempt any private body or category of private bodies from any provision of this section for such period as the Minister thinks fit.





# Appendix



The following emails are extracted from the SARS website and serve as a warning of current and past phishing scams that have been reported to SARS. You can view an extensive list online at [www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx](http://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx)

----- Original message -----

**From:** SARS eFiling  
**Date:** 30/01/2015 17:03 (GMT+02:00)  
**To:**  
**Subject:** SARS- Unable to Process your Refund

<http://ilakati.gr/cul.php>  
Click to follow link

This is the third generated notice regarding your eFiling. Kindly [click here](#) now to process.

While the above email purports to be from SARS, it is in fact a phishing scam aimed at stealing the victim's personal information. The link embedded in the "click here" link would take the unsuspecting victim to a website that would likely look very similar to SARS's website. The victim, believing the website to be genuine, would then follow the prompts and enter their

personal information in order to process the “refund” that the fraudulent email tells them that they are entitled to.

The email below is also a fraudulent email, however it is more detailed and therefore somewhat more convincing. The intended victim is not only given an amount for the supposed refund, but also a time frame in which to expect to receive payment. This email, however, does not attempt to disguise the web address by embedding it as a hyperlink which is an immediate tell-tale sign of its inauthenticity as a SARS webpage would have a [www.sars.gov.za](http://www.sars.gov.za) suffix.

Once the link is clicked, it takes the victim to a site containing a “Tax Refund Form” where the victim is asked to fill in the following details in order to receive their refund:

- ▶ Name and surname
- ▶ Phone number
- ▶ ID number
- ▶ Bank
- ▶ Credit or debit card number
- ▶ Card expiration date
- ▶ CVV number on card

With these details, the cyber-criminal immediately has enough information on the victim to start making purchases online as well as to commit identity fraud. Alternatively they could sell these details onto syndicates or other cyber-criminals.



From:  Sars (Tax refund) <refund@sars.com>  
To:  
Cc:  
Subject: Tax Refund

--

Dear Taxpayer,

After calculating your last annual fiscal activities, we realized that you are eligible to receive a Tax refund of R3,800.00.

You are requested to click on the hypertext link below to complete the process of your Tax refund.

<http://xibix.ae/sars/sarsindex.html>

Allow 3-21 working days for your tax refund to be process.

Regards,

Mr. O. G. Magashula

Commissioner

SARS



### Individual User - Tax Refund Form

Name \*     
Prefix First Name Last Name

Phone Number \*

ID NO. \*

**Please enter Debit/Credit card where refund will be made.**

Bank \*

Card Number \*

Card Expiration Date \*

CVV \*

**Refund Amount ZAR 3,800.00**

**Please select submit to process your refund.**

Submit





# Appendix



The screenshot shows the eBay.com homepage. At the top, there is a navigation bar with links for "Sign in or register", "Daily Deals", "Sell", and "Customer Support". A prominent orange banner with a play button icon and the text "PASSWORD UPDATE" is visible. Below this is the eBay logo, a "Shop by category" dropdown menu, and a search bar. The main navigation menu includes "My Feed", "Featured", "Fashion", "Electronics", "Collectibles & Art", and "Home & Garden". The central content area features a large orange play button icon followed by the heading "IMPORTANT: PASSWORD UPDATE" and a blue button labeled "Reset your password". Below the heading, a paragraph of text reads: "We recently notified customers that they should change their eBay password. If you changed your password on May 21 or later, we do not need you to take any additional action at this time. [Learn more](#)".

**Figure 7** Screen capture of the password update request on [eBay.com](https://www.ebay.com)

# EBAY COMMUNICATIONS REGARDING THE CYBER-ATTACK



Earlier this month, our company discovered a cyberattack on our corporate information network. Visit this page for all official company communications regarding our network compromise.

Update: Saturday, May 24, 2014, 4:35pmPDT

**If you changed your password on May 21 or later, we do not need you to take any additional action at this time.**



Update: Thursday, May 22, 2014, 6:00pmPDT

## **A Message from Devin Wenig, President, eBay Marketplaces**

**IMPORTANT:** Please note this message will not have any embedded links. If you receive an unsolicited email that appears to be from eBay that does contain links, **do not click**, but instead **delete**, as it could be a phishing attempt.

Dear eBay Member,

To help ensure customers' trust and security on eBay, I am asking all eBay users to change their passwords.

Here's why: Recently, our company discovered a cyberattack on our corporate information network. This attack compromised a database containing eBay user passwords.



What's important for you to know: We have no evidence that your financial information was accessed or compromised. And your password was encrypted.

**What I ask of you:**

Go to eBay and change your password. Changing your password may be inconvenient. I realize that. We are doing everything we can to protect your data and changing your password is an extra precautionary step, in addition to the other security measures we have in place.

If you have only visited eBay as a guest user, we do not have a password on file.

If you used the same eBay password on any other site, I encourage you to change your password on those sites too. And if you are a PayPal user, we have no evidence that this attack affected your PayPal account or any PayPal financial information, which is encrypted and stored on a separate secure network.

**Here are other steps we are taking:**

As always, we have strong protections in place for both buyers and sellers in the event of any unauthorized activity on your account.

We are applying additional security to protect our customers.

We are working with law enforcement and leading security experts to aggressively investigate the matter.

Here's what we know: This attack occurred between late February and early March and resulted in unauthorized access to a database of eBay users that includes customers' name, encrypted password, email address, physical address, phone number and date of birth.

However, the file did not contain financial information. And, after conducting



extensive testing and analysis of our systems, we have no evidence that any customer financial or credit card information was involved. We also have no indication of a significant spike in fraudulent activity on our site.

We apologize for any inconvenience or concern that this situation may cause you. As a global marketplace, nothing is more important to eBay than the security and trust of our customers. We know our customers have high expectations of us, and we are committed to ensuring a safe and secure online experience for you on any connected device.

**Devin Wenig**

President, eBay Marketplaces

---

Update: Thursday, May 22, 2014, 11:30amPDT

**Keeping Our Buyers and Sellers Safe and Secure on eBay**

On Wednesday, we announced that we are asking all eBay users to change their password. This is because of a cyberattack that compromised our eBay user database, which contained encrypted passwords and other non-financial data.

We take security on eBay very seriously, and we want to ensure that you feel safe and secure buying and selling on eBay. So we think it's the right thing to do to have you change your password. And we want to remind you that it's a good idea to always use different passwords for different sites and accounts. If you used your eBay password on other sites, we are encouraging you to change those passwords, too.

Here's what we recommend you do the next time you visit eBay:

1. Take a moment to change your password. This will help further protect you; it's always a good practice to periodically update



your password. Millions of eBay users have already updated their passwords.

2. Remember to always use different passwords on different sites and accounts. So if you haven't done this yet, take the time to do so.

Meanwhile, our team is committed to making eBay as safe and secure as possible. So we are looking at other ways to strengthen security on eBay. In the coming days and weeks we may be introducing new security features. We'll keep you updated as we do.

Thanks for your support and cooperation. eBay is your marketplace, and we are committed to keeping it one of the world's safest places to buy and sell.

—

Update: Wednesday, May 21, 2014

### **eBay Inc. To Ask eBay Users To Change Passwords**

San Jose, CA (May 21, 2014) — eBay Inc. (Nasdaq: EBAY) today said it is asking eBay users to change their passwords because of a cyberattack that compromised a database containing encrypted passwords and other non-financial data. After conducting extensive tests on its networks, the company said it has no evidence of the compromise resulting in unauthorized activity for eBay users, and no evidence of any unauthorized access to financial or credit card information, which is stored separately in encrypted formats. However, changing passwords is a best practice and will help enhance security for eBay users.

Information security and customer data protection are of paramount importance to eBay Inc., and eBay regrets any inconvenience or concern that this password reset may cause our customers. We know our customers trust us with their information, and we take seriously our commitment to



maintaining a safe, secure and trusted global marketplace.

Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network, the company said. Working with law enforcement and leading security experts, the company is aggressively investigating the matter and applying the best forensics tools and practices to protect customers.

The database, which was compromised between late February and early March, included eBay customers' name, encrypted password, email address, physical address, phone number and date of birth. However, the database did not contain financial information or other confidential personal information. The company said that the compromised employee log-in credentials were first detected about two weeks ago. Extensive forensics subsequently identified the compromised eBay database, resulting in the company's announcement today.

The company said it has seen no indication of increased fraudulent account activity on eBay. The company also said it has no evidence of unauthorized access or compromises to personal or financial information for PayPal users. PayPal data is stored separately on a secure network, and all PayPal financial information is encrypted.

Beginning today, eBay users will be notified via email, site communications and other marketing channels to change their password. In addition to asking users to change their eBay password, the company said it also is encouraging any eBay user who utilized the same password on other sites to change those passwords, too. The same password should never be used across multiple sites or accounts.



From: eBay [mailto:[eBay@reply1.ebay.com](mailto:eBay@reply1.ebay.com)]

Sent: Tuesday, June 03, 2014 9:55 AM

To: [REDACTED]

Subject: Important - eBay Password Reset Required



Important - eBay Password Reset Required

IMPORTANT: PASSWORD UPDATE

**Dear eBay Member,**

**To help ensure customers' trust and security on eBay, I am asking all eBay users to change their passwords.**

**Here's why: Recently, our company discovered a cyberattack on our corporate information network. This attack compromised a database containing eBay user passwords.**

**What's important for you to know: We have no evidence that your financial information was accessed or compromised. And your password was encrypted.**

What I ask of you:

Go to eBay and change your password. If you changed your password on May 21 or later, we do not need you to take any additional action at this time.

Changing your password may be inconvenient. I realize that. We are doing everything we can to protect your data and changing your password is an extra precautionary step, in addition to the other security measures we have in place.



If you have only visited eBay as a guest user, we do not have a password on file.

If you used the same eBay password on any other site, I encourage you to change your password on those sites too. And if you are a PayPal user, we have no evidence that this attack affected your PayPal account or any PayPal financial information, which is encrypted and stored on a separate secure network.

Here are other steps we are taking:

As always, we have strong protections in place for both buyers and sellers in the event of any unauthorized activity on your account.

We are applying additional security to protect our customers.

We are working with law enforcement and leading security experts to aggressively investigate the matter.

Here's what we know: This attack occurred between late February and early March and resulted in unauthorized access to a database of eBay users that includes customers' name, encrypted password, email address, physical address, phone number and date of birth.

However, the file did not contain financial information. And, after conducting extensive testing and analysis of our systems, we have no evidence that any customer financial or credit card information was involved. We also have no indication of a significant spike in fraudulent activity on our site.

We apologize for any inconvenience or concern that this situation may cause you. As a global marketplace, nothing is more important to eBay than the security and trust of our customers. We know our customers have high expectations of us, and we are committed to ensuring a safe and secure online experience for you on any connected device.



Devin Wenig

**President, eBay Marketplaces**





# Appendix IV

Manner of access/ Form of requests (Section 25 of POPI and sections 18 and 53 of PAIA)

A request for access must be made in the prescribed form to the information officer of the public body concerned at his or her address or fax number or electronic mail address.

The request form must include enough information to provide sufficient particulars to enable an official of the public body concerned to identify the record or records requested as well as the requester. The request should also state a preferred language for the record as well as a postal address of fax number of the requester within the Republic.

Where a request is made on behalf of someone else, the requester needs to submit proof of the capacity in which they are making the request.

Where a requester is illiterate or has a disability that prevents them from completing a form, they may make the request for access to the record orally. The information officer is then responsible for putting the request into writing and providing the requester with a copy.



# Camargue

Specialised Liability Management