Journal of Information Systems and Informatics
Vol. 6, No. 4, December 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i4.917 Published By DRPM-UBD

Evaluating Data Privacy Compliance of South African E-Commerce Websites Against POPIA

Adele Da Veiga[1], Hanifa Abdullah[2], Sunet Eybers[3], Elisha Ochola[4], Mathias Mujinga[5], Emilia Mwim[6]

[1,2,3,4,5,6]School of Computing, University of South Africa, Johannesburg, South Africa
Email: [1]dveiga@unisa.ac.za, [2]abdulh@unisa.ac.za, [3]eeyberss@unisa.ac.za, [4]ocholeo@unisa.ac.za, [5]mujinm@unisa.ac.za, [6]mwimen@unisa.ac.za

Abstract

South African e-commerce websites must comply with the Protection of Personal Information Act (POPIA) to process customer's personal information. However, limited research exists about data privacy implementation within these websites. This study assesses the extent of data privacy integration in 50 SA e-commerce websites. The assessment uses 57 evaluation criteria developed in the initial phases of the study, mapped to POPIA and refined in this study. While some e-commerce websites meet the requirements, significant improvements are required to safeguard users' personal information. Key areas requiring attention include processing consent, strong password management, and quality of data that was not ensured. Recommendations include clear data collection practices, explicit purpose specification, consent acquisition for processing, marketing preferences and sharing with third parties, data quality maintenance and enhanced security measures for passwords. Many online privacy policies fail to cover all POPIA privacy conditions and specific recommendations for content are included. These findings highlight a critical need for stronger data privacy practices in South African e-commerce to protect customer information. The refined evaluation criteria are a novel contribution for use by organisations to assess or develop their websites to operationalise POPIA requirements, supporting better self-assessment and integration of data privacy measures.

Keywords: Data privacy, e-commerce, websites, evaluation criteria, Protection of Personal Information Act (POPIA)

1 INTRODUCTION

The continuous advancement of information and communications technology (ICT) has resulted in a rise in online activities by both individuals and organisations. Individuals engage in online entertainment, education, finance, health, work and shopping activities, to mention a few. Technology has transformed business processes for organisations, from personnel recruitment to how products and services are offered and sold; however, this transformation is enabled using websites and mobile applications that deliver products and services

to users and customers. This online transformation is data-driven, as service providers collect and use personal information to enable and advance the provision of online services. This has given rise to the need for data privacy laws that govern how service providers can collect and use the personal information that they collect online from customers.

South Africa promulgated the Protection of Personal Information Act (POPIA) [1] in 2013, which provisions for processing personal information commencing on 1 July 2021. POPIA aims to protect personal information by introducing information protection conditions, thereby providing the minimum requirements for processing personal information to safeguard it and balance the right to access information [2]. Websites that process customers' personal information must comply with the relevant data privacy laws of the jurisdictions where personal information is processed. POPIA applies to personal information that is processed as part of an entry in a record by or for the responsible party domiciled in South Africa, or that uses automated or non-automated means situated in South Africa, thereby including the e-commerce websites of the responsible parties – which is the scope of this research study.

E-commerce websites collect various fields of personal information, allowing service providers to identify and provide the required service, which must, at the same time, meet the conditions outlined in POPIA to ensure that personal information is processed lawfully. Studies have shown that consumer concerns about privacy in e-commerce are a key challenge affecting the growth of e-commerce [3] [4]. Service providers must be aware of and implement privacy requirements to protect users from data breaches and avoid penalties for breaching regulations, which in turn will aid in establishing trust and encourage e-commerce transactions from a consumer perspective [5].

Organisations in South Africa are not yet fully compliant with POPIA and common violations towards data protection occur [6]. POPIA outlines requirements for the notification of data breaches, as well as security requirements in condition 7, which must be implemented to protect the collected data of customers. Failing to meet condition 7 of POPIA is regarded as non-compliance with the act and companies can face 10 years' imprisonment or a fine of up to R10 million. The Department of Justice and Constitutional Development in South Africa was fined R5 million South African Rands for incompliance with cyber security measures relating to an enforcement notice of the Information Regulator [6]. During the 2023/2024 period, the Information Regulator received 982 complaints and issued enforcement notices to companies like FT Rams Consulting, Dis-Chem Pharmacies, the South African Police Service (SAPS), TransUnion and the Department of Basic Education [7], [8]. South African e-commerce websites face the risk of fines, legal action, reputational damage, and loss of consumer trust if they do not comply with the conditions in POPIA.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Unfortunately, no guidance has yet been issued by the South African Information Regulator [8] on how to operationalise the conditions of POPIA on websites, and organisations are failing to address the conditions adequately.

Implementing data privacy requirements for processing personal information on websites has received attention from a research perspective. For example, Matte, Bielova and Santos [9] examined the compliance of cookie banners based on the GDPR and found that many websites had cookie banners that did not consider users' selections, thereby violating data privacy laws. Online privacy policies of South Asian websites were also assessed, with findings indicating that data privacy compliance was low, especially for protecting children's data, data retention and data transfer [10]. In South Africa, Brandreth and Ophoff [11] conducted a review of the security requirements of the top 20 e-commerce websites and identified various areas to improve the security of the websites to align with POPIA requirements and to improve consumer trust in e-commerce websites. Further studies [12][13]proposed guidelines on the content of website privacy policies to aid in meeting the data privacy requirements for websites, but found various aspects required improvement, such as data processing and consent, third-party data disclosure, certain security measures, data breach notification and data retention.

While studies have been conducted in South Africa to review the content of website privacy policies in line with data privacy requirements, there are limited studies about the current level of data privacy requirements implementation on e-commerce websites in South Africa that collect and process customer personal information online. In the absence of current data on the extent to which e-commerce websites comply with POPIA, this study aims to assess the extent to which South African e-commerce websites incorporate data privacy requirements aligned with the Protection of Personal Information Act (POPIA) and to provide targeted recommendations for improvement.

In the initial phases of this study, the researchers applied a scoping literature review to propose data privacy evaluation criteria for e-commerce websites, resulting in 22 main criteria with 57 individual evaluation criteria [14]. The criteria provide holistic guidelines to operationalise data privacy requirements on South African e-commerce websites. Although the proposed evaluation criteria serve as a point of reference to incorporate data privacy requirements on websites to align processing with the conditions of POPIA, they have not yet been tailored for practical implementation nor applied in practice to obtain a view of the current state. This study refines data privacy evaluation criteria, creating a practical framework to help organisations assess or develop their websites in line with POPIA conditions. The data privacy evaluation criteria are a unique contribution in that they present guidelines to operationalise the conditions of POPIA, supporting better self-

assessment and integration of data privacy measures to aid in compliance and protection of customer data.

1.1 Research aim

This study aims to evaluate the extent to which data privacy requirements are incorporated into SA e-commerce websites and to provide recommendations for improvement. Data privacy evaluation criteria, initially developed in the preliminary phases of this research [14], are further refined in this study for practical application to evaluate it on e-commerce websites. The data privacy evaluation criteria were developed based on best practices of operationalising the data privacy on websites and were categorised according to the conditions in POPIA. The following research questions guided this study:

RQ1: To what extent do South African e-commerce websites address the evaluation criteria for data privacy?
RQ2: What recommendations can be proposed to improve the operationalising of data privacy on South African e-commerce websites?

The outcome of the study provides insight into the extent to which data privacy aspects are addressed on e-commerce websites and identifies deficiencies to determine effective interventions for the safeguarding of customers' personal information and improved conformity with POPIA.

1.2 Background

Data privacy or data protection law regulates all stages of personal data processing [15]. Currently, over 160 countries have data privacy laws [1]. Some of the earliest data privacy laws were the Data Protection Act of Sweden which was enacted in 1973, the Privacy Act of the United States which was enacted in 1974, the Personal Data Protection Act of the Netherlands was enacted in 1975 and the Federal Data Protection Act of Germany that was enacted in 1977, with several European countries following [16]. Indonesia, Cuba, eSwatini (Swaziland), Laos and Tanzania are the countries that most recently enacted data privacy laws [16]. The European Union introduced the General Data Protection Regulation (GDPR) in May 2018, which regulates information privacy in that region [17]. In the United States, various federal and state laws deal with different aspects of data protection and privacy [18]. The EU–US Shield was approved by the European Commission in 2016 to provide a framework for transferring European citizens' personal information to the United States in transatlantic data transfers [19] which was thereafter replaced by the Trans-Atlantic Data Privacy Framework of 2022.

Data breaches have become a new reality for organisations with the increasing reliance on ICT in obtaining and sharing information through e-commerce [20]. This highlights the importance of laws for information protection and data sharing, such as the GDPR and POPIA [14] [21] [22] have been established with related legal documents such as privacy policies [23]. However, privacy laws and policies can often be complex, lengthy and ambiguous, which makes them difficult to interpret without specialised legal or technical expertise [23] [24]. The Information Regulator in South Africa has not yet provided guidelines or codes of conduct for implementing the POPIA conditions on websites.

There is a need for an improved representation of how the personal information of users is processed [23] by e-commerce websites [14] and other online services [23]. In an attempt to address this, different privacy icons and notices have been designed to indicate how personal information is processed on websites [25]. However, Rossi and Palmirani [26] maintain that the comprehensibility and effectiveness of visual representations in the form of icons and notices are questionable since most of them have not been validated. To complement the visual representation mechanisms, the Privacy by Design guidelines were developed to assist website developers in understanding how users' personal information should be processed on e-commerce websites and other designated online platforms that carry out commercial services [23]. Efforts to promote compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada have led to the development of the PIPWatch web browser toolbar. The tool was developed to assist individuals, through sharing information, to become aware of the extent to which different websites comply with the Canadian standards of legislative codes and fair information practices [27]. The development of PIPWatch helps address some limitations of privacy-enhancing technologies, such as the Platform for Privacy Preferences [27]. In the United Kingdom, researchers who worked on compliance with GDPR focused on investigating the legal compliance of cookie banners [9], which is only one aspect of the regulation.

However, website developers continue to face challenges in developing websites and policies that meet the requirements of data privacy legislation [24], underscoring the need for practical guidelines to affect the implementation of the conditions of data privacy laws to safeguard personal information processed by websites.

1.3 Protection of Personal Information Act 4 of 2013 of South Africa

The right to privacy in South Africa is addressed in Section 14 of the Constitution of South Africa 1996, the basis for data protection in South Africa [28] [29]. The legal basis for data protection in South Africa, specifically regarding safeguarding personal information with related conditions, is POPIA [30]. The Organisation

for Economic Co-operation and Development introduced the principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability [31] which were also adopted by the GDPR [32]. In South Africa, Roos [15]compared the data-protecting conditions of POPIA and the principles of the GDPR to determine the extent to which POPIA meets the minimum standards prescribed and found that although the essential provisions of POPIA that govern the processing of personal information take different approaches than those of the GDPR, POPIA provides an appropriate protection standard compared to the GDPR [15].

In 2005, POPIA was published for public comment and in November 2013 it was published in the South African Government Gazette and signed by the President of South Africa [33] [34], with Sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3) which commenced on 1 July 2020. The objective of POPIA is to protect personal information processed by public and private bodies in line with international standards and Section 14 of the Constitution of South Africa, which states that every person has the democratic right to privacy [33].

POPIA governs the collection, processing and sharing of personally identifiable information belonging to South African citizens and juristic entities [34] [35]. The Act aims to protect a data subject (the person to whom personal information applies) when a data controller (termed "responsible party" in the Act) or data processor ("operator" in the Act) processes data that pertains to the data subject and allows for the identification of the data subject [15]. Data of this nature is called personal data or personal information [15]. According to POPIA, personal information refers to information pertaining to a distinguishable, living, natural person and, where relevant, an identifiable, existing juristic person [30].

The legal ramifications of not complying with POPIA originate primarily from information security and privacy control deficits in the storage and processing of personal information, inadequacies in policies and procedures regulating personal information handling and organisations neglecting to do what is required in terms of the law for the protection of personal information [36]. Non-compliance with specific requirements of POPIA may expose both the responsible party and accompanying third parties to stringent legal punishments of up to 10 years' imprisonment or a fine of up to R10 million [36]. Complementing POPIA, PAIA addresses legal and transparent regulations that ascertain the way an entity's personal information may be accessed [37].

POPIA also applies to e-commerce websites that process personal information. Privacy policies on websites explain to customers how their personal information will be used and managed through the website [38], which must be in line with the conditions of data privacy laws such as POPIA. Privacy policies are the backbone

of present-day online privacy practices whereby organisations can pronounce their data collection and data use practices in a document that is publicly accessible [39]. A website's privacy policy is a legal document that discloses what data a website collects from its users, the manner and reason for processing the data, and the parties with whom the data are shared [32]. Additionally, the privacy policy can also outline an individual's rights concerning opting in or out of data collection, correction and deletion [32]. It can be alleged that users who engage in online services have agreed to the practices stated in the policy [39]. However, compliance with POPIA remains a significant concern [14], and websites cannot rely solely on privacy policies to address privacy requirements. They must also ensure that the data processing activities on the website effectively safeguard personal information. The absence of clear guidelines for implementing data privacy requirements on websites, coupled with limited insight into the current extent of privacy implementation, further complicates this issue. Without an understanding of whether privacy aspects are adequately addressed and which are lacking, it is difficult to assess the existing gaps or to determine effective interventions to safeguard personal information of customers that are processed on websites and to align processing with the requirements of POPIA.

1.4 Data privacy evaluation criteria for e-commerce websites

Data privacy laws provide data privacy conditions or principles that responsible parties must abide by when processing personal data. Implementing the conditions is often guided by industry standards, codes of practice or guidelines provided by information regulators. In the United Kingdom, the Information Commissioner's Office provides various guidelines, such as guidelines for sending direct marketing via electronic mail, phone, fax or post; detailed guidance for cookies; direct marketing impact assessments; and how to compile a privacy notice among various other resources provided [40]]. Similar guidance is provided for implementing the GDPR, such as guidance for remote security, a GDPR checklist, and a privacy notice [41]. In South Africa, limited guidance is available for implementing POPIA conditions on websites in terms of the content of the privacy policy, the website design and controls to be used on the website to safeguard the processing of personal information. The Information Regulator of South Africa has published some guidance relating to the processing of special personal information, specifically that of children, and the management and containment of personal information during the COVID-19 pandemic, but nothing yet about online processing of personal information. Codes of conduct are available for some industries such as banking, credit bureaus, and direct marketing. There are, however, no guidelines or codes of conduct yet in South Africa for the implementation of the POPIA conditions on e-commerce websites [42].

In the absence of guidance for operationalising data privacy conditions in e-commerce websites in South Africa, the researchers of this study, in the initial

phases of this study, proposed guidelines that e-commerce websites can use to evaluate whether their websites meet best practices for implementing data privacy conditions. Thereby providing a point of reference for the controls to be considered and guidance on operationalising the data privacy conditions of POPIA on websites [14].

A scoping literature review was used to compile a holistic set of evaluation criteria in the initial phases [14]. The criteria were derived from research published on academic databases (Web of Science, Institute of Electrical and Electronics Engineers, Association for Computing Machinery and Springer), focusing on key aspects of implementing data privacy on e-commerce websites. Given the limited studies on this topic in South Africa, the literature review included studies from various countries to provide a broader perspective in proposing the criteria. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method was applied to review the literature and extract the relevant papers that outlined existing data privacy evaluation criteria for e-commerce websites. A final list of 16 papers was included in the review to extract and propose a holistic set of evaluation criteria that can be used in South Africa and internationally. The criteria were developed by consolidating the existing academic research on the practical implementation of privacy requirements on websites, focusing on both privacy policy content and website design. Common themes were identified with sub-themes from the final list of literature papers. These themes were translated to the criteria to operationalise privacy on a website [14].

The criteria were categorised according to the conditions in POPIA and comprised 57 questions grouped into 22 categories, as listed in Table 1. POPIA includes eight conditions for the processing of personal information. It was ensured that conditions one to eight were covered in the criteria as well as four additional sections:

1. The criteria were structured according to the sections in POPIA, with Condition 1 starting at Section 8 up to Condition 8, which concludes in Section 25.
2. Sections 69 (unsolicited electronic communications), 70 and 71 (directories and automated decision making), and 72 (transborder information flows) were included as these also relate to the accountability of the responsible party.
3. An additional criterion, "Support/Awareness", was added based on a theme that was extracted from the literature review to aid consumers' data privacy support on websites.

The following sections of POPIA were excluded in the criterion:

1. Sections 26 to 35 cover the processing of special personal information and that of children, which are excluded from the scope.
2. Sections 36 to 38 apply to exemptions; Sections 39 to 54 apply to the Information Regulator; Sections 55 and 56 apply to the duties of the

Information Officer; Section 57 to 59 apply to prior authorisation and Section 60 to 68 to codes of conduct; these sections are not specific to the implementation of privacy on websites by responsible parties and were therefore not included.

3. Section 73 to 115 covers enforcement, offences, penalties, administrative fines and general provisions which are not included in the scope as it does not relate to the implementation of privacy on websites by the responsible party.

The research team reviewed the consolidated criteria, categories, questions and the mapping to POPIA through iterations to ensure the accuracy and validity of the mapping to the Act. The criteria were also mapped to the GDPR to enable further use and customisation of the criteria in other jurisdictions. This is not a complete inclusion of the GDPR principles but is limited to the scope of POPIA, which is mapped to related sections in the GDPR.

The criterion was further refined and tailored in this phase of the study before the data collection, with the following:

1. Developing answering options for each question to derive consistent data when reviewing the websites.
2. Defining for each question where the information can be obtained for the review on the website, be it as part of the login page, the user account creation or resetting, the online privacy policy or the online the terms and conditions, the website main pages or another aspect of the website such as the cookie notification.
3. Some questions were revised to ensure consistent interpretation and to allow for practical assessment on the websites.

The final criteria and questions are included in Table 2 in the Appendix. Table 2 in the Appendix shows the 22 categories categorised according to POPIA and mapped to the relevant GDPR sections. Table 2 includes a column of where on the website the information is likely to be obtained during the assessment of the criteria as well as the unique answer options that apply for each question.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 1. Data privacy evaluation criteria – main categories

Data privacy evaluation criteria	
Main criteria 1	Processing limitation – Lawfulness of processing (**Condition 1, Section 8; Condition 2, Section 9)**
Main criteria 2	Processing limitation – Minimality (**Condition 2, Section 10)**
Main criteria 3	Processing limitation – Consent, justification and objection (**Condition 2, Section 11)**
Main criteria 4	Processing limitation – Collection directly from data subject (**Condition 2, Section 12)**
Main criteria 5	Purpose specification – Collection for specific purpose (**Condition 3, Section 13)**
Main criteria 6	Purpose specification – Data subject aware of purpose of collection of information (**Condition 3, Section 13)**
Main criteria 7	Purpose specification – Retention of records (**Condition 3, Section 14)**
Main criteria 8	Further processing limitation – Further processing to be compatible with purpose of collection (**Condition 4, Section 15)**
Main criteria 9	Information quality – Quality of information (**Condition 5, Section 16)**
Main criteria 10	Openness – Notification to regulator and to data subject (**Condition 6, Section 17)**
Main criteria 11	Security safeguards – Security measures for integrity of personal information (**Condition 7, Section 19)**
Main criteria 12	Security safeguards – Information processed by operator or person acting under authority (**Condition 7, Section 20)**
Main criteria 13	Security safeguards – Security measures regarding information processed by operator (**Condition 7, Section 21)**
Main criteria 14	Security safeguards – Notification of security compromises (**Condition 7, Section 22)**
Main criteria 15	Data subject participation – Access to personal information (**Condition 8, Section 23)**
Main criteria 16	Data subject participation – Correction of personal information (**Condition 8, Section 24)**
Main criteria 17	Data subject participation – Manner of access (**Condition 8, Section 25)**
Main criteria 18	Rights of data subjects regarding unsolicited electronic communications and automated decision making – Unsolicited electronic communications (**Chapter 8, Section 69)**
Main criteria 19	Rights of data subjects regarding unsolicited electronic communications and automated decision making – Directories (**Chapter 8, Section 70)**
Main criteria 20	Rights of data subjects regarding unsolicited electronic communications and automated decision making – Automated decision making (**Chapter 8, Section 71)**
Main criteria 21	Transborder information flows – Transfers of personal information outside of the jurisdiction (**Chapter 9, Section 72)**
Main criteria 22	Support/Awareness

2 RESEARCH METHODOLOGY

2.1 Research approach

The research approach was exploratory in nature and followed a case study research strategy [43]. An embedded single-case study was applied, as adapted from [43]. The unit of analysis that was studied related to each of the 50 e-commerce websites that were evaluated to determine if they met the proposed evaluation criteria for data privacy to make recommendations for improvement. Each website was evaluated as an embedded single-case design, using the proposed criteria to evaluate the various aspects of each website. The websites that were evaluated were seen as cases that existed in their "natural setting" and real-life context and existed

before the research fieldwork and thereafter [43][43]. Research ethical clearance was obtained from the university, which required anonymising the e-commerce websites under review to preserve their privacy and confidentiality.

2.2 Sample

Purposive sampling was applied in this research, whereby specific selection criteria were applied [44]. This allowed the researchers to answer the research questions by focusing specifically on e-commerce websites in South Africa where end-users could create an online profile to facilitate the processing of personal information by the website. A drawback of purposive sampling is that the results cannot necessarily be generalised [44], but the results of this study would indicate to what extent the websites of top consumer companies incorporated data privacy conditions. The following process was applied for the sampling:

1. ChatGPT was used to obtain a list of the 50 largest consumer companies in South Africa based on revenue. The following prompt was used, "Provide a list of *the 50 largest consumer companies in South Africa based on revenue and include the source*". ChatGPT provided a list of only 43 consumer companies.
2. The researchers of this paper verified each company by confirming its website.
3. The list comprised holding companies as well as subsidiary companies of the holding companies. The researchers had to ensure that there were no duplicates on the list and searched for consumer brands on the holding company's website, verified them and, through a process of elimination, identified the consumer websites to include. Where the researchers identified duplicates, due to the inclusion of the holding companies on the list, they were removed from the list.
4. The next step focussed on verifying if the websites allowed the consumer to create an online account to purchase consumer goods. Only those websites where an online account can be created were included.
5. Websites that were not secure were not included. Some websites could not be accessed due to an unsafe browser alert, and these were excluded.
6. Only 27 of the 47 companies were retained in the final list.

To expand the sample to 50, ChatGPT was further used to obtain a list of the 25 largest South African companies based on revenue where consumers could buy technology products. The same approach was followed, and a final list of 18 technology companies was included in the sample.
The top five mobile companies in 2022 were also included in the list to derive a total of 48 company websites in the sample.

A third ChatGPT search was done for a list of the top South African companies where consumers could buy technology products to add two more companies for the final sample of 50.

The sample, therefore, comprises the top consumer companies, top technology companies and five top mobile companies in South Africa, based on revenue, that had secure websites where the end-user could create an online profile as verified by the researchers.

2.3 Data collection approach

The 50 e-commerce websites were reviewed in July and August 2023. Each researcher reviewed a selection of the e-commerce websites using the questions developed in [14]. The researchers created fictitious accounts to answer some of the questions, for example to verify what personal information was required by the website when creating an account, whether the minimality condition was applied, what the password strength requirements were, and opt-in or opt-out options were utilised by the website. The online privacy policy and website terms and conditions were consulted to answer some of the evaluation criteria questions, such as whether the purpose of data collection was specified, retention periods and transborder flow of data. Other aspects were reviewed on the website, such as whether https and cookies were used.

2.4 Data analysis approach

The data were analysed quantitatively in Excel sheets. Each researcher captured the data on an Excel template, whereafter it was screened and sanitised for analysis.

2.5 Results

The data was analysed using a frequency count of the number of occurrences of items manually captured by investigators. Table 3 provides an extract of Table 2, (See the Appendix for Table 2). The main criteria comprised various sub-criteria, which are depicted as the questions with answer options. For each question, the data was captured for the 50 websites; an overall percentage was calculated, indicating the extent to which all 50 websites met the question. For example, 98% of the websites specified in their privacy policy or online terms and conditions by whom the data are collected (under main criteria 1) and 42% of the websites captured consent at the point of collection (under main criteria 3).

The lowest score of the questions in a main criteria was used to determine the overall percentage for the main criteria. The following scale was applied to indicate the extent to which the main criteria were met:

1. Fully: 100%; indicated with the following symbol, ☺
2. Mostly: 90–99%; indicated with the following symbol, ☺
3. Partially: 50–89%; indicated with the following symbol, 😐
4. Limited: 0–49% indicated with the following symbol, ☹

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 3. Extract of criteria (full table in Appendix)

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites
Main criteria 1: Processing limitation – Lawfulness of processing (POPIA:	**Condition 1, Section 7 Condition 2 Section 8,**	**Art 5, 6, 12, 13**			
Does the website specify by whom data are collected?			Privacy policy or terms and conditions	Select one: 0 = No 1 = Yes	98%
How and where is consent captured? (Consent to agree to policy/marketing/third parties)				How and where is consent captured (at point of collection)? (Select one.) Where: 1 = Consent to the privacy policy and/or terms and conditions is required before the creation of an account.	
				2 = Consent to the privacy policy and/or terms and conditions is required at payment for product.	18%
				3 = Consent to the privacy policy and/or terms and conditions is never required.	34%

Figure 1 provides an overview of the extent to which the 50 websites addressed the criteria. Two of the 22 criteria were addressed fully (criteria 1 and 2), three mostly (criteria 5, 6 and 12), 11 partially (criteria 7, 9, 10, 13, 14, 15, 16, 17, 19, 21 and 22) and six to a limited extent (criteria 3, 4, 8, 11, 18 and 20).

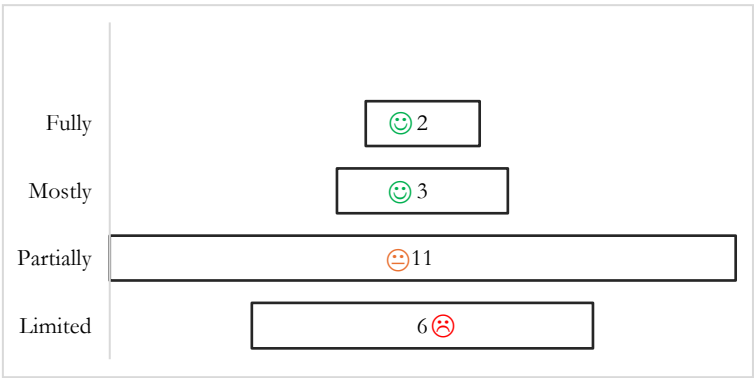

Figure 1. The extent to which the 50 websites address the evaluation criteria

The next section provides an overview of how each criterion was addressed.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Main criterion 1: Processing limitation – Lawfulness of processing (Fully)
From the data gathering, most web pages required a name (92%), surname (88%), email address (90%) and password (90%) to sign up. Although not a requirement on all the web pages, more than half of them required a mobile number (58%). No unique identifiable information, such as an identification (ID) number was requested during this stage. Most websites (98%) clearly indicated either in the privacy policy or online terms and conditions who, what and why (the reason) data were collected and how the data would be used. In general, this criterion was met. Privacy policy or terms and conditions were included on web pages and contained all the relevant information, such as the data collector, the data that were collect and the reason for collecting the data.

Main criterion 2: Processing limitation – Minimality (Fully)
All the websites collected data that were adequate, relevant and limited to what was necessary in relation to the purposes for which they were processed. The websites, therefore, met POPIA Condition 2, Section 9.

Main criterion 3: Processing limitation – Consent, justification and objection (Limited)
1. Consent privacy policy

Forty-two per cent of the websites captured consent to the privacy policy and/or terms and conditions before creating an account. Eighteen per cent of the websites captured consent to the privacy policy and/or terms and conditions when the user paid for a product, while 34% of the websites never required consent to the privacy policy and/or terms and conditions. Six per cent of the websites captured consent during the ordering of a product; consent was never captured by the rest of the websites, as it was implied when the user accessed the site and continued, as well as during account creation.
Consent to the privacy policy and/or terms and conditions was enforced using a compulsory tick box/radio button/some form of acceptance by 56% of the websites. An optional tick box/radio button/some form of acceptance to the privacy policy/terms and conditions was used by 16% of the websites. Twenty-eight per cent of the websites that were evaluated did not require consent for the privacy policy/terms and conditions.
2. Consent for marketing

Most of the websites that were evaluated (88%) obtained consent for marketing. Consent for marketing (opt-in) was partially obtained by 14% of the websites, while 50% of them provided the opportunity for consent to be revoked. Twenty per cent of the websites' consent for marketing was compulsory, while 16% of them did not ask for consent.
3. Consent for cookies

Most of the websites (62%) offered the option to manage cookies, 40% offered an optional option to accept cookies, 46% offered users no option to accept or reject cookies, and 14% collected no cookies.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

4. Consent to share with third parties

Consent to share data with third parties was partially obtained by 10% of the websites, while only 10% allowed for third-party consent to be revoked. Twenty-eight per cent of the websites enforced consent for third parties as a compulsory measure, while 52% did not ask for third-party consent. Ninety-two per cent of the websites clearly indicated whether personal information was disclosed to third parties by means of privacy policies or in terms and conditions. None of the websites indicated that they did not disclose any data. The implementation of disclosure of the types of third parties is also a concern in other studies where companies do not include sufficient information in their website privacy policies [45].

Main criterion 4: Processing limitation – Collection directly from data subject (Limited)

Forty-eight per cent of the websites collected data directly from the data subject (either through the privacy policy or terms and conditions), while 46% used a combination of collecting information directly from the data subject and receiving information from third parties. It was not clear how 40% of the websites collected information. In conclusion, this condition was met by less than half of the websites in the sample.

Main criterion 5: Purpose specification – Collection for specific purpose (Mostly)

Eighty-nine per cent of the websites explicitly defined data and the lawful purpose thereof in their privacy policy or terms and conditions. The remainder of the websites did not specify this. In conclusion, the websites partially met this criterion but improvement was required by those that did not. This finding corresponds to the most common POPIA violations where the collection purpose is not specified in privacy policies [6].

Main criterion 6: Purpose specification – Data subject aware of purpose of collection of information (Mostly)

Eighty-nine per cent of the websites took steps to ensure that the data subject was made aware of the purpose of collection in either the privacy policy or the terms and conditions. In conclusion, this condition was met by the majority of the websites but improvement was required by those that did not. Purpose specification was also a concern in a study conducted in Japan, where at least 20% of the privacy policies under review did not specify the purpose of collecting personal information [45].

Main criterion 7: Purpose specification – Retention of records (Partially)

Sixty-four per cent of the websites contained information about the retention of records in the privacy policy or terms and conditions. In conclusion, the record retention specifications of the websites required improvement. Research has found

that the GDPR requirement for the storage period is not covered in privacy policies by 40-45% of websites in the EU [46], indicating that this non-compliance is also prevalent in countries that have had data privacy laws for various years.

Main criterion 8: Further processing limitation (Limited)
Only 20% of the websites stated that they would obtain consent from the data subject if their data would be subjected to further processing. In conclusion, this criterion was not met, as the majority of the websites did not state that they would obtain consent for further processing.

Main criterion 9: Information quality (Partially)
Only fifty-two per cent of the websites had controls, which could lead to capturing higher quality data enforced from pre-populated items, by using dropdown boxes, validations, etc. In conclusion, this criterion was not met, as almost half of the websites did not include controls to ensure that personal information was complete, accurate and not misleading.

Main criterion 10: Openness – Notification to regulator and to data subject (Partially)
Most of the websites (96%) had a privacy policy or terms and conditions information on the website, with only 6% of the websites not having their privacy policy accessible on every page on the website. Not all the websites that were evaluated had a privacy notice at the point of data collection (28%), while the majority (72%) had a notice in place. Most of the websites (98%) had a link to their terms and conditions and privacy policy. In conclusion, this criterion was mostly met.

Main criterion 11: Security safeguards – Security measures for integrity of personal information (Limited)
All the websites that were evaluated used a secure connection and had a valid https certificate. The majority of the websites required passwords to contain numbers (62%), followed by a combination of upper- and lower-case letters (58%), symbols like "? $ % ^ & (56%), and nine or more characters long (52%); 8% specified a password requirement of between four and 20 characters long, while an eight character long password was adequate for 50% of the websites. Surprisingly, 20% of the websites allowed passwords to be less than eight characters long, and 8% did not specify and enforce any password requirements. Only 24% of the websites that were evaluated used a password strength indicator to guide the user in setting strong passwords. Therefore, there was room for improvement in enforcing and guiding strong user passwords, the condition was generally highlighted as non-compliant. The main reason for the status was the lack of multi-factor authentication on most websites when the user logged on, while almost half of the websites required users to verify personal information when signing up or resetting a password. Furthermore, the specification of strong passwords was not enforced

on almost half of the web pages, while only 38% of accounts were locked after entering an incorrect password. This was an opportunity for hackers to attempt to access user accounts through trial and error. In line with that, 64% of the websites that were evaluated allowed unlimited attempts to enter the wrong credentials before the account was locked. This is in line with a study conducted in South Africa that also found strong password management is not applied consistently on websites (e.g. not enforcing minimum length, limiting incorrect attempts, locking accounts) [11]. Studies about GDPR compliance found that not all websites address data safeguards and this remains an issue to improve [46].

Main criterion 12: Security safeguards – Information processed by operator or person acting under authority (Mostly)
Most of the websites that were evaluated (94%) referred to sharing data with third parties in their privacy policy or terms and conditions.

Main criterion 13: Security safeguards – Security measures regarding information processed by operator (Partially)
Seventy-eight per cent of the websites stated third-party categories or the type of company that would be processing information on the website or in their privacy policy or terms and conditions.

Main criterion 14: Security safeguards – Notification of security compromises (Partially)
An alarming 48% of the websites that were evaluated did not indicate if data subjects would be informed if their personal information was compromised in the privacy policy or terms and conditions. This was, therefore, indicated as an area for improvement which is also one of the most common POPIA violations where organisations fail to inform data subjects and Information Regulator if there was data breach [6].

Main criterion 15: Data subject participation – Access to personal information (Partially)
Only 74% of the websites specified how users could access personal stored data. Only 54% of the websites allowed access to data, free of charge, while 10% offered access to data for a fee payable. Thirty-six per cent of the websites that were evaluated did not provide any information on access to personal information. Eighty-six per cent of the websites that were evaluated allowed users to review or access data collected. Most of the websites did not offer free access to stored personal data and, as such, improvement was required for this criterion.

Main criterion 16: Data subject participation – Correction of personal information (Partially)
Eighty-eight per cent of the websites that were evaluated provided users with the functionality to correct data. Seventy per cent of the websites provided users with

the functionality to delete data. The majority of the websites, therefore, complied with this condition. However, those that did not require improvement. Similarly, a study of South Asian websites found that website privacy policies do not include how data can be updated or deleted [10].

Main criterion 17: Data subject participation – Manner of access (Partially)
Seventy-eight per cent of the websites that were evaluated disclosed the process for data subject access requests in terms of other applicable regulatory requirements such as PAIA. Although there was room for improvement, most of the websites complied with this criterion. This is in line with findings in the South Asian study where most website privacy policies in that review also did not include information about how customers can request copies of their personal information that was collected by the company [10].

Main criterion 18: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Unsolicited electronic (Limited)
Only 46% of the websites that were evaluated offered users the option to manage, edit and delete subscriptions through, for example, a marketing preference centre where users could make changes/selections. Of the 46% of the websites that offered users the option to manage, edit and delete subscriptions, 22% had pre-ticked boxes confirming marketing consent. This was, therefore, identified as an area for improvement. This is still an area of frustration for consumers in South Africa in that personal information is used for direct marketing without the necessary consent [6].

Main criterion 19: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Directories (Partially)
Only 2% of the websites that were evaluated informed data subjects before their information was included in a physical or online directory, free of charge. Seventy-four per cent of the websites did not mention or explain any rights of data in online or physical data directories to data subjects, while 24% contained information about online data storage in the physical or online directories but did not inform data subjects of the inclusion free of charge. This was, therefore, identified as an area of improvement.

Main criterion 20: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Automated decision making (Limited)
Only 10% of the websites that were evaluated explained how the automatic processing of data from data subjects would affect them, while 24% did not mention or explain any rights of data subjects. This was, therefore, an area for improvement. Similar results were found in a study in the EU where the automated

profiling requirement of the GDPR were only met by 28.5% of companies in that study [46].

Main criterion 21: Transborder information flows – Transfers of personal information outside the South Africa (Partially)
Only half of the websites that were evaluated included an explanation on how transborder information flows of the data subject's data and the effect on the data subject. Therefore, this area had room for improvement.

Main criterion 22: Support/Awareness (Partially)
Only 58% of the sign-up pages that were evaluated on the websites contained prompts such as password strength indicators to assist users to create strong passwords. Forty-two per cent of the websites did not offer any prompts. Most indicators on the web pages (88%) did not offer additional information via links to privacy policies or terms and conditions.

Most of the web pages offered help resources to users through the information contained in the privacy policy (96%), followed by a helpline (phone number or call centre) (92%). Other popular help resources included email (78%), social media (for example, Twitter or Facebook) 74% and frequently asked questions (FAQs) (70%). Less popular methods were the availability of a chatbot (24%), WhatsApp (32%) and fax, contact form and a specific application (40%). It was alarming to note that only 58% of the websites offered users guidance on creating strong passwords and did not offer additional information on creating strong passwords via links to privacy policies or terms and conditions (88%). Despite the availability of help resources, which were predominantly available through the privacy policy and helpline, security awareness was an area earmarked for improvement. Studies have shown that website privacy policies are not read by users and that these policies are often lengthy and difficult to understand [47]. This emphasises the need to provide support functions on the website to aid users in navigating through the privacy policy and understanding how their information will be processed.

3 RECOMMENDATIONS

Table 4 provides a summary of the results of the 22 data privacy evaluation criteria for e-commerce websites and a summary of the key recommendations. The recommendation discussion is formulated in line with the findings in the main categories and addresses the gaps identified in each category with a status of either "limited" or "partially".

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 4. Data privacy evaluation criteria for e-commerce websites results and summary of recommendations

Data privacy evaluation criteria	Status		Summary of recommendations
Main criteria 1: Processing limitation – Lawfulness of processing	Fully	☺	-
Main criteria 2: Processing limitation – Minimality	Fully	☺	-
Main criteria 3: Processing limitation – Consent, justification and objection	Limited	☹	Websites to capture consent prior to or at the point of creation of a user account or payment. Websites to obtain consent for marketing and allow for management of marketing preferences. Websites to allow for the management of cookie preferences. Websites to allow for the management of third-party sharing of data.
Main criteria 4: Processing limitation – Collection directly from data subject	Limited	☹	Privacy policies to specify collection methods.
Main criteria 5: Purpose specification – Collection for specific purpose	Mostly	☺	Privacy policies to specify the purpose of data collection and processing.
Main criteria 6: Purpose specification – Data subject aware of purpose of collection of information	Mostly	☺	Privacy policies and website to specify the purpose for data collection and processing.
Main criteria 7: Purpose specification – Retention of records	Partially	😐	Privacy policies to include information about the retention of records.
Main criteria 8: Further processing limitation – Further processing to be compatible with purpose of collection	Limited	☹	Privacy policies to specify information and processes for further processing.
Main criteria 9: Information quality – Quality of information	Partially	😐	Websites to include controls to ensure complete, accurate and not misleading collection of data e.g. dropdown boxes and validations.
Main criteria 10: Openness – Notification to regulator and to data subject	Partially	😐	Websites to have a privacy policy/notice that is accessible on the website.
Main criteria 11: Security safeguards – Security measures for integrity of personal information	Limited	☹	Websites to enforce the use of strong passwords. Websites to incorporate strong password management controls, e.g. lockout of accounts after incorrect attempts, security questions, multi-factor authentication and use of CAPTCHA's.
Main criteria 12: Security safeguards – Information processed by operator or person acting under authority	Mostly	☺	Privacy policies to include information about sharing data with third parties.
Main criteria 13: Security safeguards – Security measures regarding information processed by operator	Partially	😐	Privacy policies to include information about the categories of third parties with whom data is shared.
Main criteria 14: Security safeguards – Notification of security compromises	Partially	😐	Privacy policies to include information about notification in the event of a data breach.

Data privacy evaluation criteria	Status		Summary of recommendations
Main criteria 15: Data subject participation – Access to personal information	Partially	😐	Privacy policies to include information about the process to access data.
Main criteria 16: Data subject participation – Correction of personal information	Partially	😐	Privacy policies to include information about the process for correcting and deleting data.
Main criteria 17: Data subject participation – Manner of access	Partially	😐	Privacy policies to include the process for data subject access requests.
Main criteria 18: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Unsolicited electronic communications	Limited	☹	Websites to include marketing preference management.
Main criteria 19: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Directories	Partially	😐	Privacy policies to include information use of personal data in online/physical directories where applicable.
Main criteria 20: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Automated decision making	Limited	☹	Privacy policies to include information about electronic communications and automated decision-making.
Main criteria 21: Transborder information flows – Transfers of personal information outside the South Africa	Partially	😐	Privacy policies to include information about transborder flows that are applicable.
Main criteria 22: Support/Awareness	Partially	😐	Websites to include help resources e.g. FAQs, Helpline, chatbot, social media and other contact information to seek help.

Note: Fully 100%; Mostly 90–99%; Partially 50–89%; and Limited 0–49% (Percentages for each criteria are included in the Appendix in Table 2)

The first set of recommendations is channelled to categories 3 and 4, which deal with "processing limitation". Regarding category 3, it is recommended that all websites comply with the provisions of Section 11 of POPIA regarding the issue of consent, justification and objection concerning the personal information of the data subject. For category 4, it is recommended that all websites act in accordance with the provisions of Section 12 of POPIA while collecting data by ensuring that all personal information is collected directly from the data subject.

The second set of recommendations is directed at categories 5, 6 and 7, which concern "purpose specification" being "partially" met. Referring to category 5, it is recommended that, in accordance with the provisions of Section 13 (1) of POPIA, all websites must specify the purpose for which personal information is collected, which must be lawful. Concerning category 6, it is recommended that the websites that are not in compliance must ensure that the data subject is mindful of the purpose for collecting the personal information, as specified in Section 13 (2) of POPIA. In terms of category 7, it is recommended that all websites ensure

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

that their actions are consistent with Section 14 of POPIA regarding the retention of records of personal information.

The third recommendation only concerns category 8, which deals with "further processing to be compatible with purpose of collection". This category has the status of "limited", which indicates that most websites fail to obtain consent from the data subject for further processing of personal information. It is, therefore, recommended that further processing of personal information by the websites must be consistent with the purpose for which the information is collected in the first place, as stated in the provisions of Section 15 of POPIA.

The fourth recommendation is directed at only category 9, which relates to "information quality". It has the status of "partially", showing that many websites do not contain measures to ensure that personal information is of the required quality. It is, therefore, recommended that all websites should take the necessary steps to ensure that the personal information is complete, accurate and not misleading, while simultaneously maintaining the purpose for which the personal information is collected in terms of Section 16 (1) and (2) of POPIA.

The fifth recommendation is channelled specifically to category 10, which deals with the issue of "openness". The status of this category is "partially", which demonstrates that the requirement is met by most websites, but there is still room for improvement. Therefore, it is recommended that all websites be open by ensuring that the data subject is aware of all the information specified in Section 18 of POPIA.

The sixth set of recommendations is directed at categories 11, 12, 13 and 14, which concern "security safeguards". Both categories 11 and 14 have the status of "limited", category 13 has the status of "partially" and category 12 has the status of "mostly". Category 11 has the status of "limited", which concerns the "security measures on integrity of personal information". It is recommended that the responsible party takes the necessary steps to secure the integrity and confidentiality of personal information under its care, as specified in Section 19 of POPIA. For category 14, with the status of "limited", which concerns the "notification of security compromise", it is recommended that the responsible party must, in terms of Section 22 of POPIA, notify the regulator and the data subject where there is a reasonable suspicion of security compromise. Regarding category 13 with the status of "partially", which concerns "security measures regarding information processed by operator", it is recommended that in accordance with the provision of Section 21 of POPIA, a responsible party must ensure that the operator acting on its behalf adheres to the required security measures when processing personal information. Category 12 has the status of "mostly", which concerns "information processed by operator or person acting under authority". For this category, it is recommended that such a person should

process the information with the knowledge or authorisation of the responsible party in terms of Section 20 of POPIA.

The seventh set of recommendations deals with categories 15, 16 and 17, which concern "data subject participation". While category 15 has the status of "limited", categories 16 and 17 have the status of "partially". Regarding category 15, which deals with "access to personal information", it is recommended that a data subject must have access to personal information as provided in Section 23 of POPIA. Concerning category 16, which deals with "correction of personal information", it is recommended that a provision be made for a data subject to be allowed to request a responsible party to correct or delete personal information in accordance with the provision of Section 24 of POPIA. Then, regarding category 17, which concerns "manner of access", it is recommended that the requirement of access to information in terms of PAIA must be followed as indicated in Section 25 of POPIA.

The eighth set of recommendations is channelled towards categories 18, 19 and 20, which deal with the "rights of data subjects regarding unsolicited electronic communications and automated decision making". Categories 18 and 20 have the status of "limited", while category 19 is "partially". Concerning category 18, which deals with "unsolicited electronic communications", it is recommended that all websites should comply with the provision of Section 69 of POPIA by preventing the processing of personal information of a data subject for the purpose of direct marketing. Regarding category 20, which concerns "automated decision making", it is necessary that all websites comply with Section 71 of POPIA by ensuring that the automated processing of personal information may not expose data subject to decisions that could have legal consequences. Then, concerning category 19, which deals with "directories", it is recommended that the subject data should be notified before personal information is included in the directory, and subject data must be given an opportunity to object to such use of personal information as stated in section 70 of POPIA.

The ninth recommendation is channelled to category 21, which deals with the issue of "transborder information flows". The status of this category is "partially" which demonstrates that most websites meet the requirement but there is still room for improvement. Section 72 of POPIA states that no responsible party is allowed to transfer a data subject's personal information to a third party residing in a foreign country.

Finally, the tenth recommendation is directed at category 22, which deals with the issue of "support and awareness". The status of this category is "partially", and it is shown that there is a need for improvement, especially in security awareness.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

4 DISCUSSION

This study set out to answer the following research question: *To what extent do South African e-commerce websites address the evaluation criteria for data privacy?* The researchers assessed 50 South African e-commerce websites using the proposed evaluation criteria. In answering the research question, it was shown that most of the criteria were not met and that there are inconsistencies in data privacy implementation across the assessed websites. The websites only complied fully with two sections of the guidelines, e.g., in collecting data that were adequate, relevant and limited to what was necessary in relation to the purposes for which they were processed.

The study confirms the need for improvements in implementing data privacy requirements on South African e-commerce websites. The findings are in line with studies conducted in other jurisdictions that found the processing of personal information on websites does not adequately meet data privacy requirements. A study conducted in Japan found that 90% of websites' privacy policies do not adequately address data retention, how personal information will be processed, user rights, and security measures [45]. Research on Finnish public sector web services revealed inconsistencies between privacy policies and actual data practices, indicating a lack of transparency in how personal data is handled [48]. Their study raised the need for improved awareness of data privacy regulations and how to implement them on websites, which is not only a need in that jurisdiction, but also in South Africa. Jurisdictions such as the European Union (EU), with a heavy stance towards data privacy, still face challenges towards compliance, with studies underscoring a gap between the legal requirements for data privacy compliance and the actual practices of many websites. In the EU, websites, for example, still fail to comply with all the conditions of the GDPR, highlighting the ongoing challenge of websites in ensuring adherence to data privacy legislation [46].

This research addressed the second research question, *RQ2: What recommendations can be proposed to improve the operationalising of data privacy on South African e-commerce websites?* by outlining the criteria that were not addressed with a summary of recommendations. The recommendations can be implemented from two main approaches. Firstly, updating the websites' privacy policy content is essential as this will address most of the identified gaps. The website privacy policies must address all POPIA conditions. Specific attention should be given to the current lacking aspects, by including the specification of collection methods, outlining the process to obtain consent for further processing, defining retention periods, listing categories of third parties with whom information is shared, and detailing procedures for accessing and correcting data, automated decision making, transborder flows. Privacy policy content alignment with data privacy law requirements can be improved through the use of Large Language Models (LLM), which can aid in the efficiency of assessing compliance of privacy policies with legal requirements by incorporating the criteria as part of prompts of LLMs [49].

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

The second approach involves reviewing and updating the processing of personal information on websites, which requires web developers to consider these aspects in the website's design. Areas for improvement include methods for obtaining consent for processing, marketing preferences and sharing information with third parties at the point of collection as well as the management of cookie preferences. While consent is a requirement across data privacy legislation, websites still fail to adequately address it [47], emphasising the need for improvement of data privacy on websites and the need for coherent guidelines.

This study recommends that South African e-commerce websites must be designed to ensure the collection of accurate and complete information and incorporate controls for robust password management controls, which are not consistently implemented across all websites. Additionally, websites must provide easy access to the privacy policies and include additional support and awareness resources regarding customer information processing.

This study contributes by practically verifying the extent to which South African e-commerce websites met the evaluation criteria for implementing data privacy guidelines. This is a pointer to industry stakeholders (e.g., website designers) to ensure that data collected from a data subject, either directly or via a third party, is done in compliance with the data requirements. While progress is being made, South African e-commerce websites still have room for improvement in implementing data privacy requirements. The study's findings present organisations with the current state of the implementation of data privacy criteria and a point of reference to improve which can be included in data privacy strategies and plans. It is recommended that the evaluation criteria for data privacy be used as a checklist or self-assessment in determining if a website meets the expectations of data privacy requirements as part of website development and improvement. The evaluation criteria can further be applied across different industries or jurisdictions for comparison and to monitor the status of the implementation of data privacy criteria.

Consumers can only trust e-commerce websites when processing their personal information if their privacy and security are considered [11]. If the consumers' personal information is not protected, it could negatively affect their trust in the organisation [50]. Privacy policies should have a positive influence on consumers' trust in the e-commerce organisation [11], but should be complete and address the conditions of POPIA to indicate to the customer their commitment and concern for the privacy of the customers' personal information. Studies have shown that if consumers' trust in the e-commerce website improves, then it can lead to an increased willingness to purchase online [51], whereas if the trust relationship is affected negatively, the customer's data is not protected. Addressing the recommendations can aid in meeting the POPIA conditions as well as contribute

to the trusting relationship between consumers and e-commerce websites in South Africa.

A limitation of the study is that the included sample represents only 50 e-commerce websites in South Africa and does not include all industries. Future research can extend the study to a larger sample to also include websites that process special personal information (e.g. religion, race, health) or personal information of children, which will then include Sections 26 to 35 of POPIA that were excluded in the scope of this study. This study did not include data from websites with restricted access requiring a subscription, which may have affected the comprehensiveness of the results and can be included in future research for a more complete assessment of the current state of website compliance towards POPIA. A further limitation is that the review is subjective at a point in time, and quantitative follow-up studies are recommended. It is also recommended that LMMs be used for a more in-depth legal review of privacy policy in alignment with data privacy law requirements.

The evaluation criteria provide best practices for data privacy implementation on websites but should not be regarded as a review of legal compliance with a specific data privacy act. The evaluation criteria are not a review of the technical security controls of the websites but only focus on the requirements listed in the Appendix with practical operational guidance. Future research can incorporate legal compliance and technical security reviews of websites to expand the criteria.

5 CONCLUSION

This study aimed to assess the extent to which 50 South African e-commerce websites addressed data privacy evaluation criteria. The review indicated that several of the evaluation criteria were not implemented, and there were various inconsistencies across the websites. The findings confirm the need for improvement in the implementation of data privacy requirements across South African e-commerce websites to improve compliance with POPIA as well as to contribute to a trusting relationship between consumers and e-commerce websites. This study provided a valuable and novel contribution by analysing the current posture of implementing data privacy conditions and providing recommendations to enhance the state of implementing data privacy conditions on South African e-commerce websites. The 56 questions provide a valuable framework for organisations to guide them in operationalising the conditions of POPIA on their websites to protect consumer data. Future research can focus on expanding the evaluation criteria to include a legal and security review and examine the data privacy requirements of a larger sample and possibly of different industries. The use of LLM to assist in reviewing privacy policies' content should also be investigated to incorporate the POPIA conditions and evaluation criteria for a more efficient evaluation of compliance. It will also be of value to repeat the

evaluation of the websites over time in a longitudinal study to monitor the status of compliance.

REFERENCES

[1] G. Greenleaf, "Global data privacy laws 2023: 162 national laws and 20 bills," *Privacy Laws and Business International Report*, vol. 181, no. 1, pp. 1–4, 2023, doi: 10.2139/ssrn.4426146.

[2] South African Government, "Protection of Personal Information Act No. 4 of 2013.," 2013. Accessed: Oct. 22, 2023.

[3] Z. Wu, S. Shen, H. Zhou, H. Li, C. Lu, and D. Zou, "An effective approach for the protection of user commodity viewing privacy in e-commerce website," *Knowl Based Syst*, vol. 220, no. 2021, p. 106952, 2021, doi: 10.1016/j.knosys.2021.106952.

[4] R. Bandara, M. Fernando, and S. Akter, "Privacy concerns in e-commerce: A taxonomy and a future research agenda," *Electronic Markets*, vol. 30, no. 3, pp. 629–647, 2020, doi: 10.1007/s12525-019-00375-6.

[5] A. Eckert, G. S. Milan, G. Roy, and R. Bado, "Welcome back: Repurchase intention of Brazilian customers on e-commerce websites," *Revista de Ciências da Administração*, vol. 23, no. 59, pp. 106–120, May 2021, doi: 10.5007/2175-8077.2021.e69913.

[6] Legalese, "What are the Most Common POPIA Violations," Legalese, 2024. Accessed: Nov. 14, 2024.

[7] S. Mzekandaba, "InfoReg slaps TransUnion with enforcement notice," IT Web, 2024. Accessed: Nov. 14, 2024.

[8] Information Regulator South Africa, "Information Regulator South Africa: Enforcement notices," Information Regulator South Africa, 2024. Accessed: Nov. 14, 2024.

[9] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework," *In Proceedings of IEEE Symposium on Security and Privacy*, vol. 2020-May, pp. 791–809, 2020, doi: 10.1109/SP40000.2020.00076.

[10] Y. Javed, K. M. Salehin, and M. Shehab, "A study of South Asian websites on privacy compliance," *IEEE Access*, vol. 8, pp. 156067–156083, 2020, doi: doi.org/10.1109/ACCESS.2020.3019334.

[11] D. Brandreth and J. Ophoff, "Investigating customer-facing security features on South African e-commerce websites," in *Information and Cyber Security: 19th International Conference, ISSA 2020*, Springer Science and Business Media Deutschland GmbH, 2020, pp. 144–159. doi: 10.1007/978-3-030-66039-0_10.

[12] A. Vorster and A. da Veiga, "Proposed guidelines for website data privacy policies and an application thereof," in *International Symposium on Human Aspects of Information Security and Assurance*, Skovde: Springer Nature Switzerland, Jul. 2023, pp. 192–210. doi: 10.1007/978-3-031-38530-8_16

[13] J. Maraba and A. Da Veiga, "A study of online privacy policies of South African retail websites," in *International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability*, Madrid: Springer Nature Switzerland, Oct. 2023, pp. 426–440. doi: 10.1007/978-3-031-48855-9_32.

[14] A. Da Veiga, E. Ochola, M. Mujinga, and E. Mwim, "Investigating data privacy evaluation criteria and requirements for e-commerce websites," in *Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2022. Communications in Computer and Information Science*, M. F. Guarda, T., Portela, F., Augusto, Ed., Springer, Cham, 2022, pp. 297–307. doi: 10.1007/978-3-031-20316-9.

[15] A. Roos, "Data protection principles under the GDPR and the POPI Act: A comparison," *THRHRS*, vol. 86, no. February 2023, pp. 1–26, 2023.

[16] G. Greenleaf, Global tables of data privacy laws and bills (8th Ed.), 2023

[17] M. Goddard, "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact," *International Journal of Market Research*, vol. 59, no. 6, pp. 703–705, 2017, doi: 10.2501/ijmr-2017-050.

[18] C. Murray, "U.S. data privacy protection laws: A comprehensive guide," Forbes. Accessed: Mar. 20, 2024.

[19] European Commission, "European Commission launches EU-U.S. privacy shield: Stronger protection for transatlantic data flows." Accessed: Mar. 20, 2024.

[21] G. Greenleaf, "Global data privacy laws 2019: 132 national laws & many bills," *Privacy Laws & Business International Report*, vol. 2019, no. 157, pp. 14–18, 2019, doi: 10.2139/ssrn.4426146.

[22] A. Gurung and M. K. Raja, "Online privacy and security concerns of consumers," *Information and Computer Security*, vol. 24, no. 4, pp. 348–371, 2016, doi: 10.1108/ICS-05-2015-0020.

[23] S. Barth, D. Ionita, and P. Hartel, "Understanding online privacy - A systematic review of privacy visualizations and privacy by design guidelines," *ACM Comput Surv*, vol. 55, no. 3, 2022, doi: 10.1145/3502288.

[24] F. Pereira, P. Crocker, and V. R. Q. Leithardt, "PADRES: Tool for PrivAcy, Data REgulation and Security," *SoftwareX*, vol. 17, p. 100895, 2022, doi: 10.1016/j.softx.2021.100895.

[25] G. Fox, C. Tonge, T. Lynn, and J. Mooney, "Communicating compliance: Developing a GDPR privacy label," in *In Proceedings of the 24th Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, 2018, pp. 1–5.

[26] A. Rossi and M. Palmirani, "A visualization approach for adaptive consent in the European data protection framework," *Proceedings of the 7th International Conference for E-Democracy and Open Government, CeDEM 2017*, pp. 159–170, 2017, doi: 10.1109/CeDEM.2017.23.

[27] A. Clement, D. Ley, T. Costantino, D. Kurtz, and M. Tissenbaum, "The PIPWatch toolbar: Combining PIPEDA, PETs and market forces through social navigation to enhance privacy protection and compliance," in *In Proceedings of 2008 IEEE International Symposium on Technology and Society,* IEEE, 2008, pp. 1–10. doi: 10.1109/ISTAS.2008.4559759.

[28] D. Basimanyane, "The regulatory dilemma on mass communications surveillance and the digital right to privacy in Africa: The case of South Africa.," *African Journal of International and Comparative Law* , vol. 30, no. 3, pp. 361–382, 2022, doi: 10.3366/ajicl.2022.0414.

[29] Constitution of the Republic of South Africa, "South African Government," 1996. Accessed: Oct. 22, 2023.

[30] South Africa Government, "Protection of Personal Information Act No. 4 of 2013.," 2013. Accessed: Oct. 22, 2023.

[31] Organisation for Economic Co-operation and Development (OECD), "The OECD Privacy Framework. Technical Report. OECD." Accessed: Oct. 22, 2023.

[32] I. Wagner, "Privacy Policies Across the Ages: Content of Privacy Policies 1996–2021.," *ACM Transactions on Privacy and Security*, vol. 26, no. 3, pp. 1–32, 2023.

[33] P. J. de Waal, "The Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA): It is time to take note.," *Current Allergy & Clinical Immunology*, vol. 35, no. 4, pp. 232–236, 2022.

[34] M. Katurura and L. Cilliers, "Privacy in wearable health devices: How does POPIA measure up?," in *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems*, 2019, pp. 112–122. doi: 10.29007/qsp7.

[35] E. Raaff, N. Rothwell, and A. Wynne, "Aligning South African data and cloud policy with the POPI Act," in *International Conference on Cyber Warfare and Security*, 2022, pp. 279–287. doi: 10.34190/iccws.17.1.19.

[36] T. Moabalobelo, S. Ngobeni, B. Molema, P. Pantsi, M. Dlamini, and N. Nelufule, "Towards a Privacy Compliance Assessment Toolkit," in *2023 IST-Africa Conference (IST-Africa)*, IEEE, 2023, pp. 1–8.

[37] South African Government, "Promotion of Access to Information Act 2 of 2000," 2000.

[38] R. Amos, G. Acar, E. Lucherini, M. Kshirsagar, A. Narayanan, and J. Mayer, "Privacy policies over time: Curation and analysis of a million-document dataset," in *Proceedings of the Web Conference 2021* , 2021, pp. 2165–2176.

[39] J. Tang, H. Shoemaker, A. Lerner, and E. Birrell, "Defining privacy: How users interpret technical terms in privacy policies," in *Proceedings on Privacy Enhancing Technologies*, 2021. doi: 10.2478/popets-2021-0038.

[40] Information Commissioner's Office, "Information Commissioner's Office - For organisations." Accessed: Aug. 21, 2023.
[41] GDPR.EU, "GDPR.EU." Accessed: Aug. 21, 2023.
[42] Information Regulator of South Africa, "Information Regulator (South Africa_," Guidance notes. Accessed: Aug. 21, 2023.
[43] R. K. Yin, *Case study research - Design and Methods*, 3rd ed. Thousand Oaks, California: SAGE Publications, 2002.
[44] M. Saunders, P. Lewis, and A. Thornhill, *Research methods for business students*, Seventh ed. England: Pearson Education Limited, 2016.
[45] K. Mori, T. Nagai, Y. Takata, and M. Kamizono, "Analysis of Privacy Compliance by Classifying Multiple Policies on the Web," in *Proceedings - 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1734–1741. doi: 10.1109/COMPSAC54236.2022.00276.
[46] T. Al Rahat, M. Long, and Y. Tian, "Is Your Policy Compliant? A Deep Learning-based Empirical Study of Privacy Policies Compliance with GDPR," in *WPES 2022 - Proceedings of the 21st Workshop on Privacy in the Electronic Society, co-located with CCS 2022*, Association for Computing Machinery, Inc, Nov. 2022, pp. 89–102. doi: 10.1145/3559613.3563195.
[47] X. Lin, H. Liu, Z. Li, G. Xiong, and G. Gou, "Privacy protection of China's top websites: A Multi-layer privacy measurement via network behaviours and privacy policies," *Comput Secur*, vol. 114, Mar. 2022, doi: 10.1016/j.cose.2022.102606.
[48] T. Heino, R. Carlsson, S. Rauti, and V. Leppänen, "Assessing discrepancies between network traffic and privacy policies of public sector web services," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2022. doi: 10.1145/3538969.3539003.
[49] T.-H.-G. Vu and X.-B. Hoang, "User Privacy Risk Analysis within Website Privacy Policies," Institute of Electrical and Electronics Engineers (IEEE), Sep. 2024, pp. 1–6. doi: 10.1109/mapr63514.2024.10660854.
[50] J. Kim, R. L. Baskerville, and Y. Ding, "Breaking the Privacy Kill Chain: Protecting Individual and Group Privacy Online," *Information Systems Frontiers*, vol. 22, no. 1, pp. 171–185, Feb. 2020, doi: 10.1007/s10796-018-9856-5.
[51] I.-D. Anic, V. Škare, and I. Kursan Milaković, "The determinants and effects of online privacy concerns in the context of e-commerce," *Electron Commer Res Appl*, vol. 36, p. 100868, Jul. 2019, doi: 10.1016/j.elerap.2019.100868.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Appendix

Table 2. Data privacy evaluation criteria for e-commerce websites – questions and results

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
Main criteria 1: Processing limitation – Lawfulness of processing (POPIA:	**Condition 1, Section 8, Condition 2 section 9**	**Art 5, 6, 12, 13**				
What personal information is required to sign up? (To assess if more information is required for purchasing than what is necessary for the objective)			Sign up page	List the personal information: (Select ALL that apply that is COMPULSORY) 1 = Name	92%	Fully
				2 = Surname	88%	
				3 = Username	12%	
				4 = Email	90%	
				5 = Password	90%	
				6 = Cell	58%	
				7 = Tax/VAT	10%	
				8 = Identity type	14%	
				9 = Passport	4%	
				10 = ID number	8%	
				11 = Other (Specify)	32%	
Does the website specify by whom data are collected?			Privacy policy or terms and conditions	Select one: 0 = No 1 = Yes	98%	
Does the website explain what data will be collected?			Privacy policy or terms and conditions	Select one: 0 = No 1 = Yes	98%	
Does the website clarify why data will be collected?			Privacy policy or terms and conditions	Select one: 0 = No 1 = Yes	98%	
Does the website explain how the collected data will be used?			Privacy policy or terms and conditions	Select one: 0 = No 1 = Yes	98%	
Main criteria 2: Processing limitation – Minimality	**Condition 2, section 10**	**Art. 5**	**Data collection**	**Answer options**	**%**	**Status**
The data collected are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed? (No unnecessary data are collected) (in the context of creating an account/buying a product)			Sign-up page	Select one: 0 = No 1 = Yes	100%	Fully
Main criteria 3: Processing limitation – Consent, justification and objection	**Condition 2, section 11**	**Art. 5, 7, 18, 21**	**Data collection**	**Answer options**	**%**	**Status**

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
How and where is consent captured? (Consent to agree to policy/marketing/third parties)			Website	How and where is consent captured (at point of collection)? (Select one.) Where: 1 = Consent to the privacy policy and/or terms and conditions is required before the creation of an account.	42%	Limited
				2 = Consent to the privacy policy and/or terms and conditions is required at payment for product.	18%	
				3 = Consent to the privacy policy and/or terms and conditions is never required.	34%	
				4 = Other	6%	
			Website, cookie, terms and conditions, policy	Consent for marketing is obtained (either in a cookie/radio button/separate consent tick box/terms and conditions of acceptance, etc). Select one: 0 = No 1 = Yes	88%	
			Website (sometimes notification banner)	Management of cookies is available on the website: (Select one. 0 = No	38%	
				1 = Yes (reject, accept, change options)	62%	
				2 = Other	0%	
			Website (sometimes notification banner)	Acceptance of cookies is required. (Select one.) 0 = Optional	40%	
				1 = Compulsory (no option to accept/reject)	46%	
				2 = No cookies	14%	
			Website	How: Consent to the privacy policy and/or terms and conditions is: (Select one.) 1 = Compulsory tick box/radio button/some acceptance to privacy policy/terms and conditions	56%	
				2 = Optional tick box/radio button/some acceptance to privacy	16%	

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
				policy/terms and conditions		
				3 = No consent required for privacy policy/terms and conditions (*create an account/add product to shopping basket)	28%	
Can consent be partial or revoked? (Consent for agree to policy/marketing/third parties)			Website	Consent for privacy policy/terms and conditions: (Select ALL that applies.) 1 = Partial (consent for some items and not others)	6%	
				2 = Can be revoked (withdrawn)	2%	
				3 = All fields compulsory	62%	
				4 = Consent not asked	30%	
			Website	Consent for marketing (opt in) (Select ALL that applies.) 1 = Partial	14%	
				2 = Can be revoked	50%	
				3 = Compulsory	20%	
				4 = Consent not asked	16%	
			Website	Consent for third parties (Select ALL that applies.) 1 = Partial	10%	
				2 = Can be revoked	10%	
				3 = Compulsory	28%	
				4 = Consent not asked	52%	
Is granular consent included for different types of processing?			Website	Select one: 0 = No 1 = Yes	4%	
Does the website clarify if personal information will be disclosed to a third party?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	92%	
Does the website explain under what conditions the data will be disclosed to third parties?			Privacy policy/ terms and conditions	Select one: 0 = No	8%	
				1 = Yes	92%	
				2 = Not applicable – do not disclose to third parties	0	
Main criteria 4: Processing limitation – Collection directly from data subject	**Condition 2, section 12**	**Art. 13**	**Data collection**	**Answer options**		
Does the website collect information directly from			Privacy policy/	Select one: 0 = No – only from third parties	2%	Limited

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
the data subject and not via third parties?			terms and conditions	1 = Yes – directly from data subject	48%	
				2 = Combination – data subject and receive your information from third parties	46%	
				3 = Do not know	4%	
Main criteria 5: Purpose specification – Collection for specific purpose	**Condition 3, section 13**	**Art. 5**	**Data collection**	**Answer options**		
Is a specific, explicitly defined and lawful purpose specified?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	98%	Mostly
Main criteria 6: Purpose specification – Data subject aware of purpose of collection of information	**Condition 3, section 13**	**Art. 13**	**Data collection**	**Answer options**		
Are steps taken on the website to ensure that the data subject is aware of the purpose of collection?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	98%	Mostly
Main criteria 7: Purpose specification – Retention of records	**Condition 3, section 14**	**Rec. 65**	**Data collection**	**Answer options**		
Is the retention of records specified?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	64%	Partially
Main criteria 8: Further processing limitation – Further processing to be compatible with purpose of collection	**Condition 4, section 15**	**Rec. 50**	**Data collection**	**Answer options**		
Does the website state that it will obtain consent from the data subject if their data will be subject to further processing?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	20%	Limited
Main criteria 9: Information quality – Quality of information	**Condition 5, section 16**	**Art. 5**	**Data collection**	**Answer options**		
Are website controls included to ensure that the personal information collected is complete, accurate and not misleading (dropdown boxes, validations, etc.)?			Account creation page and shopping cart (address/ phone for example)	Select one: 0 = No 1 = Yes	52%	Partially
Main criteria 10: Openness – Notification to regulator and to data subject	**Condition 6, section 17,18**	**Art. 12, 13**	**Data collection**	**Answer options**		
Is there a privacy policy on the website?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	96%	Partially

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
Is the privacy policy accessible via every page on the website?			Website	Select one: 0 = No 1 = Yes	94%	
Is there a privacy notice at the point of data collection (e.g., when the online account is created)?			Website	Select one: 0 = No 1 = Yes	72%	
Is there a link to terms and conditions and the privacy policy on the website (any page)?			Website	Select one: 0 = No 1 = Yes	98%	
Main criteria 11: Security safeguards – Security measures for integrity of personal information	**Condition 7, section 19**	**Art. 5, 32, 35**	**Data collection**	**Answer options**		
Does the website use https? (Is the connection secure?)			URL	Select one: 0 = No 1 = Yes	100%	Limited
Is the https certificate valid?			URL lock check	Select one: 0 = No 1 = Yes	100%	
What is the password (if any) strength requirements?			Sign-up page	Select all that apply: 0 = Less than 8 characters long	20%	
				1 = 8 characters long	50%	
				2 = 9 and more characters long	52%	
				3 = Use upper- and lower-case letters	58%	
				4 = Numbers	62%	
				5 = Symbols like ! " ? $ % ^ &	56%	
				6 = No requirements	8%	
				7 = Strength indicator (e.g., weak/strong)	24%	
				8 = Other	4%	
Does the account get locked after entering the incorrect password? After how many attempts?			Log-in page	Does the account get locked out? Select one: 0 = No 1 = Yes	38%	
			Log-in page	After how many attempts does the account lock out? (Select one.) 1 = 3 attempts	26%	
				2 = 4–5 attempts	10%	
				3 = unlimited attempts	64%	
Is there a forgot password option? Is there an option to change the password?			Log-in page	Forgot password: (Select one.) 0 = No 1 = Yes	100%	
			User account page	Change password: (Select one.) 0 = No 1 = Yes	76%	
What are the password requirements when changing passwords?			Resetting password page	Select all that apply: 0 = Less than 8 characters long	18%	
				1 = 8 characters long	52%	

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
				2 = 9 and more characters long	50%	
				3 = Use upper- and lower-case letters	56%	
				4 = Numbers	62%	
				5 = Symbols like ! " ? $ % ^ &	52%	
				6 = No requirements	10%	
				7 = Strength indicator (e.g., weak/strong)	20%	
				8 = Other	2%	
How is the password reset (i.e., use of account recovery questions, new password autogenerated, link provided to change password or OTP sent)?			Resetting password page	Select all that apply: 1 = Use of account recovery questions	0%	
				2 = New password autogenerated	4%	
				3 = Link provided to change password sent to email	64%	
				4 = OTP sent	12%	
				5 = Click change password link, new page provided to type in password (dedicated password change page, no other controls)	24%	
				6 = Other	0	
What are the communication options when resetting a password (email, SMS, app, etc.)?			Resetting password page	Select all that apply: 0 = None	32%	
				1 = Email	66%	
				2 = SMS	10%	
				3 = Website	0	
				4 = call	0	
				5 = App on phone, etc	2%	
				6 = Other	0	
Is multi-factor authentication offered?			Log-on page	Select one: 0 = No (only a password)	96%	
				1 = Yes (more than only a password)	4%	
What multi-factor authentication settings are available?			Log-on page	Select all that apply: 1 = Password	2%	
				2 = Pin	2%	
				3 = N/A	96%	
				4 = Other	0	
Is a CAPTCHA (e.g., words/image/picture to proof you are not a robot) used for authentication?			Log-on page	Select one: 0 = No 1 = Yes	78%	
Are users required to verify any information (e.g., email address)? How is this done?			Sign-up page/ password reset page	Select one: 0 = No 1 = Yes	48%	
Are cookie consent statements included to reject all, accept all or change settings? (This			Pop up?	See Q9 – DUPLICATE		

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
does not refer to the terms and conditions to alert you to the fact that the website uses cookies, but rather giving options to revise the cookies).						
Does the website clarify that it takes steps to provide security for collected data?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	92%	
Does the website state that unauthorised access to users' personal data will be prevented?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	90%	
Main criteria 12: Security safeguards – Information processed by operator or person acting under authority	**Condition 7, section 20**	**Art. 29**	**Data collection**	**Answer options**		
Does the website refer to sharing data with third parties? *			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	94%	Mostly
Main criteria 13: Security safeguards – Security measures regarding information processed by operator	**Condition 7, section 21**	**20 Art. 29**	**Data collection**	**Answer options**		
Are third-party categories (type of company) named on the website or in the privacy policy?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	78%	Partially
Main criteria 14: Security safeguards – Notification of security compromises	**Condition 7, section 22**	**Art. 33, 34**	**Data collection**	**Answer options**		
Does the website indicate that data subjects will be informed if their personal information was compromised?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	52%	Partially
Main criteria 15: Data subject participation – Access to personal information	**Condition 8, section 23**	**Art. 13-15, 20**	**Data collection**	**Answer options**		
Does the website specify how the user can access their data?			PAIA request, privacy policy, terms and conditions	Select one: 0 = No 1 = Yes	74%	Partially
Is data access requests free of charge?			Policy on website	Select one: 0 = No	10%	
				1 = Yes	54%	
				2 = Not stated	36%	
Does the website allow users to review/access collected data? (User provided data, not applicable to system data like IP)			Use account	Select one: 0 = No 1 = Yes	86%	

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
Main criteria 16: Data subject participation – Correction of personal information	**Condition 8, section 24**	**Art 5, 16, 17, 19**	**Data collection**	**Answer options**		
Does the website provide for means for the data subject to correct data?			User account, privacy policy, terms and conditions	Select one: 0 = No 1 = Yes	88%	Partially
Does the website provide for means for the data subject to delete data? (Right to be forgotten)			User account, privacy policy, terms and conditions	Select one: 0 = No 1 = Yes	70%	
Main criteria 17: Data subject participation – Manner of access	**Condition 8, section 25**	**Art.13-15**	**Data collection**	**Answer options**		
Is the process for data subject access requests specified in terms of other applicable regulatory requirements (e.g. Promotion of Access to Information Act (PAIA) process in South Africa)?			Website legal space, privacy policy, terms and conditions, PAIA manual	Select one: 0 = No 1 = Yes	78%	Partially
Main criteria 18: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Unsolicited electronic communications	**Chapter 8, section 69**	**Rec. 70**	**Data collection**	**Answer options**		
Does the website include a marketing **preference centre** to manage, edit and delete subscriptions? (Does the website have a f**acility to make changes/selections** (e.g., tick box with options to change marketing preferences)? (This question does not relate to notifying the data subject that marketing is taking place, thus not the content of the policy or terms and conditions.)			Account creation/log in	Select one: 0 = No 1 = Yes	46%	
If you answered Q57 with a "yes", then proceed to answer Q58 and select either option 0, 1 or 2. If you selected "No" for Q57, then select N/A = 3 for Q58: Boxes are pre-ticked for marketing consent. (Does the website have a facility to make changes – e.g.,			Account creation/log in	Select all that apply: 0 = No, not pre-ticked	18%	
				1 = Yes, pre-ticked	22%	
				2 = Compulsory tick	0%	
				3 = N/A (No boxes/preference centre to select choices)	54%	

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
tick box with options to change marketing preferences?)						
Main criteria 19: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Directories	**Chapter 8, section 70**	-	**Data collection**	**Answer options**		
If the website compiles a directory of personal information, does the website inform the data subject free of charge and before the information is included in a physical or online directory?			Privacy policy/ terms and conditions	Select one: 0 = No	12%	Partially
				1 = Yes	2%	
				2 = No mention thereof	74%	
Main criteria 20: Rights of data subjects regarding unsolicited electronic communications and automated decision making – Automated decision making	**Chapter 8, section 71**	**Art. 22**	**Data collection**	**Answer options**		
Is there an explanation for how the automatic processing of data of a data subject will affect the data subject?			Privacy policy/ terms and conditions	Select one: 0 = No	33%	Limited
				1 = Yes	10%	
				2 = No mention thereof	24%	
Main criteria 21: Transborder information flows – Transfers of personal information outside the South Africa	**Chapter 9, section 72**	**Art 44-50**	**Data collection**	**Answer options**		
Is there an explanation for how transborder information flows of data of a data subject takes place and how it will affect the data subject?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	50%	Partially
Main criteria 22: Support/Awareness	-	-	**Data collection**	**Answer options**		
Are there any security prompts (e.g., password strength indicators)?			Sign-up page for password	Select one: 0 = No 1 = Yes	58%	Partially
Are security indicators explained in more detail or are there links for additional information?			Privacy policy/ terms and conditions	Select one: 0 = No 1 = Yes	22%	
What are the various types of help resources available?			Website	Select ALL that apply: 1 = Privacy policy	96%	
				2 = FAQ privacy/security/user data	70%	
				3 = Helpline (phone number/call centre)	92%	
				4 = Chatbot	24%	
				5 = WhatsApp	34%	

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Criteria and questions	POPIA mapping	GDPR mapping	Data collection	Answer options	% of all 50 websites	Status
				6 = Email	78%	
				7 = Social media (e.g. ,Twitter, Facebook)	74%	
				8 = Other	40%	

Note: For Yes/No questions, only the Yes % is given.