Vorster, Armand, and Adéle da Veiga. "Proposed Guidelines for Website Data Privacy Policies and an Application Thereof." *International Symposium on Human Aspects of Information Security and Assurance*. Cham: Springer Nature Switzerland, 2023.
https://link.springer.com/chapter/10.1007/978-3-031-38530-8_16

Pre-Print Version

Proposed guidelines for website data privacy policies and an application thereof

Armand Vorster[1][0009-0000-3819-1592] and Adéle da Veiga[1][0000-0001-9777-8721]

School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
dveiga@unisa.ac.za
armandvorster93@gmail.com

Abstract. Business-to-consumer (B2C) e-commerce websites have recently increased in South Africa. The extent of addressing privacy requirements in B2C e-commerce websites is still in its infancy in South Africa with the Protection of Personal Information Act which only came into effect recently. A scoping literature review was conducted to define a holistic set of privacy policy guidelines for websites. In total, 14 privacy policy guidelines for websites were identified to aid website owners in developing their online data privacy policies. The research design further included a sample of ten popular South African B2C e-commerce website privacy policies using an embedded single-case study design to illustrate the application of the guidelines and to establish the extent of the content of the sample of website privacy policies in terms of the proposed privacy policy guidelines. The findings indicated that the website privacy policies did not fully address the proposed guidelines. The proposed privacy policy guidelines for websites provide website owners with a way to assess and improve their privacy policy content to contribute to compliance with data privacy requirements and to build consumer trust.

Keywords: privacy policy, websites, B2C, e-commerce, websites, guidelines, South Africa, POPIA

1 Introduction

Online shopping through electronic commerce (e-commerce) is widely popular in South Africa; it is estimated that more than half of frequent internet users in South Africa make purchases over the internet [1], [2]. One of the reasons for this is ever-increasing internet growth in South Africa [2]. Each of these e-commerce websites should, in turn, have a website privacy policy; this is an online document that describes how a given company or organisation will manage, acquire, apply and distribute the personal data of customers [3]. The contents of a website privacy policy should comply with data privacy requirements, since consumers' personal information is stored and processed on e-commerce websites [4].

The Protection of Personal Information Act (POPIA) of South Africa defines a set of eight conditions that serve as the basic requirements to ensure that user data privacy

is maintained [5]. POPIA does not explicitly list guidelines or criteria that must be included in a website privacy policy; but provides privacy conditions. Various studies have been conducted to define guidelines of criteria for website privacy policy content [6]–[8], however, most of these studies focus on international regulations for data privacy compliance, which might not always apply to a South African environment. Furthermore, a holistic set of guidelines are not available and different criteria or requirements are proposed by various studies. Therefore, it is valuable to explore the guidelines for website privacy policy content for South African organisations, to provide website owners guidance to refer to, which can aid in complying with POPIA and improve the protection of personal information.

With the increase in e-commerce and the advent of POPIA, it is important, from a regulatory perspective, that e-commerce websites are compliant with the Act [1]. It has also been shown that an increase in consumer trust will lead to increased purchases on e-commerce websites [9]. This has been known for a long time, and privacy policies can be used to increase the trust level of end-users [10], [11]. For example, research by Eckert et al. [9] demonstrated the beneficial impact of trust on the repurchase probability of customers on online shopping websites. Furthermore, research conducted by Malapane [12] found that trust in online shopping in South Africa is vital and that solid regulations and policies are required to reduce the perceived risk many South Africans have about the online shopping e-commerce environment. Therefore, maintaining a high trust level between the consumer and the e-commerce website is essential. Research has also suggested that negatively perceived privacy concerns, such as the invasion of privacy experienced by consumers in the e-commerce environment, can lead to reduced trust levels [13]. It has also been found that consumer trust levels can be increased by inserting correct and accurate privacy information in a website privacy policy [11].

2 Research Problem

POPIA provides a condition-based approach to regulating personal information requirements; however, there is a lack of detail provided in the Act regarding the application of these conditions [14]. Consequently, there are currently no distinct privacy policy guidelines or criteria for South African B2C e-commerce websites. This is concerning, as it is evident from the literature reviewed that privacy plays a vital role in consumer trust levels, and it has been shown that high levels of trust may lead to an increase in e-commerce sales [9]. A study by Aladeokin et al. [15] also found that many websites based in the Commonwealth countries, including South Africa, do not conform to the privacy compliance recommendations set out in their study. A large amount of research has been done on the privacy aspects that must form part of a website's privacy policy [7], [8], [16]. However, these studies focus on specific governmental privacy policies; for example, Tesfay et al. [17] compiled a so-called 'PrivacyGuide' for internet privacy policies focussed on the General Data Protection Regulation (GDPR), which is legislation for the European Union (EU). The use of e-commerce is increasing in South Africa, and a study done by Steyn et al. [18] found

that South Africans will opt for e-commerce sites because they are convenient, but that the websites must guarantee the protection of personal data. Mofokeng [19] also showed that customer loyalty towards e-commerce websites would increase if trust for these websites were to increase. Privacy and the trust of consumers are directly linked to each other; if privacy is low, then consumer trust will also be low [13].

3 Background

3.1 Privacy

Privacy is the term used to determine what level of personal information is shared with an organisation or any other person; it also relates to when and how this information will be shared [20]. The capability of individuals to control what information is shared is becoming increasingly important. In an age where social media and the internet are part of our daily lives, organisations need to understand the privacy perceptions of individuals if they are to maintain their trust [21].

3.2 The POPI Act

POPIA was promulgated in 2013 but was implemented in South Africa only in July 2021. The Act's function is to aid the protection of personal data that is processed by public and private operators [22]. POPIA consists of eight conditions that provide guidance on implementing the Act; these eight conditions must be met when personal information is processed in South Africa [23]. If POPIA is not correctly applied, it may lead to imprisonment and fines being issued to the guilty party [23].

3.3 Privacy Policies and Consumer Privacy Concerns

An online privacy policy informs consumers about the privacy practices implemented by the specific company's website; the legislation or standards used by companies may vary from site to site [24]. Recently more people have become concerned about how their online data is being used by organisations, as the reporting on this matter has increased in the past few years [25]. According to Brunotte et al. [26], users feel that privacy policies are not always transparent on how personal information will be processed and used. One of the major concerns is the fact that privacy policies are typically lengthy documents, and many users don't even read them. Kretschmer et al. [27] mention that fewer than one out of 600 people bothered to read website privacy policies in the year 2018. The length of a privacy policy directly impacts its significance [28]. Some users have suggested that they do not read privacy policies due to the complexity and the legal language used [29]. A study, spanning more than twenty years, was conducted on more than one million privacy policies by Amos et al. [30], using an automated tool. It was found that privacy policies are becoming larger and more challenging to comprehend and lack transparency regarding third-party user details and technologies that track users. Reinhardt et al. [31] mention that visual representations of privacy policies can be used to increase the understanding and attractiveness of privacy policies while reducing the amount of text.

Another concern is that privacy policies are not always straightforward, transparent and easily understood. Kotal et al. [32] note that this vagueness can be found frequently in privacy policies. In a study done by Proctor et al. [33], it was found that even college students may have problems interpreting and understanding the content of website privacy policies. However, various steps and guidelines can be applied to increase the readability and usability of privacy policies [34], [35]. Privacy policies might not always comply with all governmental requirements, Zaeem and Barber [36] found that some of the websites they reviewed did not meet all the GDPR requirements. Furthermore, it has been found that certain websites do not follow and adhere to the privacy policy statements as set out on the website [37]. Evidence has emerged of governments in African countries requesting online personal data of users without following privacy norms and standards [38]. Worldwide data breaches are still occurring, even with the implementation of more regulations and legislation to protect personal data [39]. For example, a study was done during the Covid-19 pandemic on residents of Buffalo City Municipality in South Africa; it was found that many residents experienced cybercrime associated with online shopping [40]. Additionally, Mutemwa et al. [41] highlighted the problem of increasing cyberattacks and concerns that developing countries like South Africa should be dealing with threats posed by cyberattacks. In an analysis done by van Ooijen and Vrabec [42] it was found that internet governance structures like the GDPR can increase user control. It is, therefore, vital for privacy policies to address data privacy requirements, to be easy to comprehend, and to promote user control, all of which can reduce data breaches and user privacy concerns.

4 Research Methodology

4.1 Design of Literature Review

A scoping review methodology was selected as it is explanatory and can provide clarification on main concepts [43], focusing on the broader coverage of the literature rather than the detailed depth of the literature [44], examining and mapping emerging evidence on a topic [45]. The PRISMA method was used in conjunction with the literature review, as it ensures that a systematic review is accurate and inclusive. The PRISMA method is based on a 27-item checklist; with guidance on each item of the checklist [46]. The outcome of the scoping review was the privacy guidelines.

4.2 Databases and Search Method

Four primary databases were selected for this study, the databases were; ACM, IEEE Xplore, ScienceDirect and SAGE Journals. Only English journals and conference papers published between 2016 and 2022 were selected to ensure that the latest privacy guidelines were reflected. The search terms included a combination of the following words and phrases: (a) “Website Privacy policy principles”; (b) “Website privacy policy requirements”; (c) “Website privacy policy criteria”; (d) “Elements of a website privacy policy”; (e) “Websites AND privacy compliance”. A total of 78 unique articles were found. The first screening step was to remove any duplicate articles found; this

was done using Mendeley. Within the initial 78 articles, Mendeley did not detect any duplicates. The second screening was a manual screening, where the titles and abstracts of the articles were examined to determine if the articles were suitable for full-text analysis. This was done by searching for similar keywords, as listed above. In this screening, 46 articles were excluded for not matching the research search terms and research objective, and one was excluded for not meeting the timeline requirements. After the second screening, only 31 articles remained, and these were selected for the full-text analysis. The articles chosen for the full-text analysis were carefully studied in the eligibility screening phase, the main inclusion criteria being that the paper should provide guidelines for the content of online privacy policies. The final count of articles to be included in the study was 11.

4.3 Website Privacy Policy Guidelines

The 11 articles were reviewed to compile the holistic website privacy policy guidelines, the results are depicted in Table 1. Some of the guideline names were adjusted to be more inclusive of the guidelines used in the articles. The columns with a tick indicate which privacy guidelines were included in each of the final 11 reviewed articles. Each privacy guideline was also mapped to the relevant POPIA condition. The guidelines are equally important, as each can be linked to at least one POPIA condition. Not one of the studies focuses on a research study done in a South African context, nor uses POPIA as a guideline. See Appendix A for a description of the proposed guidelines and related 24 questions that can be used to assess website privacy policy content.

Table 1. Summary of website privacy policy guidelines

[1]**Privacy Policy Guidelines**	[47]	[48]	[49]	[50]	[51]	[7]	[27]	[37]	[52]	[53]	[54]	**Total**	[2]POPIA Condition
(1)			√		√	√		√		√	√	6	Condition 1
(2)	√					√						2	Condition 7
(3)	√		√	√		√			√	√		6	Condition 4
(4)	√					√			√	√	√	5	Condition 5
(5)	√			√	√	√		√	√	√	√	8	Condition 2
(6)	√		√	√	√	√			√	√		7	Condition 2
(7)	√		√	√		√	√	√				6	Condition 3
(8)	√		√			√		√	√			5	Condition 7
(9)		√	√	√	√	√	√	√		√	√	9	Condition 6
(10)								√				1	Condition 6
(11)		√		√		√	√		√			5	Condition 6
(12)	√		√	√		√			√		√	6	Condition 4
(13)	√	√	√	√		√	√	√		√	√	9	Condition 8
(14)					√	√		√				3	Condition 6

[1]**Privacy Policy Guidelines:** (1) Assurances, (2) Breach Notification (Accountable), (3) Cross-border Data Transfer and Portability, (4) Accuracy of Data, (5) Data Collection Sources and Purpose, (6) Data Processing and Consent, (7) Data Retention, (8) Data Security Measures, (9) Disclosure of Privacy Policy, (10) Transparency and Ease of Access, (11) Entity, (12) Third-Party Data Users and Disclosure of Personal Data, (13) User Control, (14) Clarity of Privacy Policy

[2]**POPIA**: Condition 1 (Accountability), Condition 2 (Processing limitation), Condition 3 (Purpose Specification), Condition 4 (Further Processing Limitation), Condition 5 (Information Quality), Condition 6 (Openness), Condition 7 (Security Safeguards), Condition 8 (Data subject participation)

4.4 Research Approach

A single-case study research methodology was chosen; case studies provide a holistic view of an occurrence being studied or observed [55]. This is ideal for this research, as it can be used to study a phenomenon linked with a real-life context, where the boundaries between the phenomenon and the context are not transparent or evident [56], [57]. The single phenomenon to be studied was whether the sample of South African B2C e-commerce website privacy policies include the proposed guidelines. A single website's privacy policy was studied as an embedded single-case design, where each embedded unit of analysis represented a specific website's different privacy policy. The identity of the sample websites was anonymised. Ethical clearance for this research was obtained from the university. The website privacy policies were anonymised to protect the identity and confidentiality of these organisations, in line with the research ethical clearance.

4.5 Research Strategy and Sampling

The sample size for a case study is usually small [58]. According to Lenz [59], the minimum sample size that can be used for a single-case study is one. Also, it is not typically the goal of a case study to generalise a population statistically [57], [60]. Therefore, when the population size chosen for a case study is small, it is not ideal to use random sampling techniques [60], [61]. For this reason, a non-random sampling technique was selected for this study. Popular B2C e-commerce websites in South Africa were determined by using the following search strings on an online search engine: (a) "top e-commerce websites South Africa"; (b) "popular e-commerce website South Africa"; (c) "top 10 e-commerce sites South Africa". A combined list of 10 e-commerce websites was selected from different search results. To justify the popularity of the B2C e-commerce websites selected, each website's company was searched on Twitter. If the company of the specific B2C e-commerce website did not have more than 5 000 Twitter followers, the company was not included on the list.

4.6 Data Analysis

This research followed a quantitative data analysis method to assess the different website privacy policies. The majority of the proposed guidelines can be answered by "yes" or "no" questions. If a specific privacy policy guideline is not fully addressed, then it is regarded as not met. For example, the User Control guideline requires three sub-conditions to be met in the form of three questions as per Appendix A, if any sub-condition is not met, then the privacy policy does not meet the guideline User Control.

Two of the guidelines do not have "yes" or "no" answers. The *Clarity of the Privacy Policy* guideline focuses on the privacy policy readability level and ensures that the privacy policy is not too long and tedious. The readability of a privacy policy can be measured using a Flesch Reading Ease Score (FRES); from here, it can be determined whether the privacy policy is comprehensible [35], [62], [63]. The FRES system is well known for evaluating legal documents, and it works on a 100-point scale; the lower the score, the higher the difficulty level of the text. In addition, the Flesch Grade Level (FGL) can also be used to determine how comprehensible text is, indicating the US

grade-school level similarity of the text being read [63]. A study done by Srinath et al. [64] on more than one million English website privacy policies from more than 800 top-level domains (TLD), found the following averages for privacy policies; (a) an average word length of 1410.88; (b) a FRES score of 40.32; (c) a Flesh-Kincaid Grade level of 14.42. For the guideline *Transparency or Ease of Access*, the number of "clicks" it takes to get to the privacy policy from the website home page will be recorded. The purpose of this guideline is to see how difficult it is to get to the website's privacy policy from the home page, without the assistance of the cookie or consent pop-up.

5 Results

Table 2 depicts the evaluation of the content of the sample of website privacy policies in terms of the proposed guidelines in Table 1. The first column lists the privacy guidelines, the next columns define the "yes" or "no" for meeting the proposed guidelines for each website privacy policy.

Table 2. Data of the privacy policy guidelines evaluation

Website Privacy Policy Guidelines	**Privacy Policies of Websites 1 -10**										**Total Yes**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Entity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	10
Disclosure of Privacy Policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	10
Clarity of the Privacy Policy (FRES Scores)	40.8	42.7	49.1	44.5	43.7	44.8	42.7	41.5	38.9	38.4	N/A
Transparency or Ease of Access (No. of Clicks)	1	1	1	1	1	2	2	1	N/A	2	N/A
Data Collection Sources and Purpose	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	10
Data Processing and Consent	No	No	No	Yes	No	No	Yes	No	No	No	2
Cross border data transfer and Portability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	10
Third-Party Data Users and Disclosure of Personal Data	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes	No	6
User Control	No	No	No	Yes	No	No	No	Yes	No	No	2
Data Security Measures	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	8
Breach Notification (Accountable)	No	No	No	No	Yes	No	Yes	No	No	No	2
Assurances	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	8
Data Retention	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	7
Accuracy of Data	No	No	Yes	Yes	Yes	No	No	No	Yes	No	4

For each guideline, a maximum of 10 "yes" answers are possible, as one "yes" answer per privacy policy is possible. Not one of the 10 websites analysed achieved a complete score for addressing all the guidelines. Table 3 summarises the key findings for the websites not meeting the guidelines.

Table 3. Findings for not meeting the website privacy policy guidelines

Website privacy policy guidelines	Findings for not meeting the website privacy policy guidelines	[3]Number
Data Processing and Consent	When accessing the website, a consent pop-up notification is available with the privacy policy, but the consent for data processing is not defined in the privacy policy.	2
	When accessing the website, a pop-up notification is available, together with the privacy policy, but consent is not requested from the data subject.	2
	When accessing the website, a pop-up notification is available together with the privacy policy, but consent is not requested from the data subject. Secondly, the privacy policy does not define consent for data processing.	1
	No cookies or consent pop-ups when accessing the website.	1
	No cookies or consent pop-ups when accessing the website and the consent for data processing is not clearly defined in the privacy policy.	2
Third-Party Data Users and Disclosure of Personal Data	The roles of the third party(s) are not discussed.	4
User Control	Data sharing and processing are not controllable by the data subject.	8
Data Security Measures	No information is provided on the security measures of third parties regarding data transfer.	2
Breach Notification (Accountable)	No breach notification section in the policy.	3
	Steps to notify the information regulator of a breach are not mentioned.	1
	The data subject will not be notified about a data breach, the data subject must request this information.	1
	The breach notification section is available, but the steps to notify the information regulator of a breach are not mentioned.	3
Assurances	No details provided about POPIA or the information regulator.	2
Data Retention	Data retention information is provided, but the data retention period details are unavailable.	2
	No data retention information is provided.	1
Accuracy of Data	It is not mentioned whether the privacy policy is up to date, and no "last update" date is provided in the policy.	6
[3]*Number of privacy policies that scored "No"*		

Table 4 analyses the guidelines *Clarity of the Privacy Policy* and *Transparency or Ease of Access* which could not be answered by a simple "yes" or "no answer". The total word count of each privacy policy is shown, together with the FRES and FGL scores. To better interpret these scores and word counts, they are compared to the averages found in the research of Srinath et al. [64] by evaluating the percentage deviation from the known averages. Readable.com was used to calculate the FRES and FGL scores, as this is one of the most popular websites for calculating these scores [65]. The lower the FRES score, the higher the difficulty level of reading and understanding the text; hence the colour green (*) is assigned to positive deviation values (higher FRES scores) and orange (**) or light green (**) to negative deviation values (lower FRES scores). For the FGL measurement, the lower the FGL score, the lower the difficulty level of reading and understanding the text; hence the colour green (*) is assigned to negative deviation values and orange (**) or light green (**) to positive

deviation values. In other words, constructive results are marked with (*) and negative results with (**).

Table 4. Analysis of privacy policy guidelines; Clarity of the Privacy Policy and Transparency or Ease of Access

Privacy Policy	FRES Score	FGL Score	Word Count	% Deviation from average FRES score of *40.32* [64]	% Deviation from average FGL score of *14.42* [64]	% Deviation from average Word Count of *1410.88* [64]	[4]Clicks
1	40.8	12	2528	1.19 *	-16.78 *	79.18 **	1
2	42.7	11.2	2424	5.9 *	-22.33 *	71.81 **	1
3	49.1	10.9	3850	21.78 *	-24.41 *	172.88 **	1
4	44.5	10.9	2955	10.37 *	-24.41 *	109.44 **	1
5	43.7	10.3	2507	8.38 *	-28.57 *	77.69 **	1
6	44.8	10	2451	11.11 *	-30.65 *	73.72 **	2
7	42.7	10.3	5645	5.9 *	-28.57 *	300.1 **	2
8	41.5	10.2	1565	2.93 *	-29.26 *	10.92 **	1
9	38.9	12.4	1418	-3.52 **	-14.01 *	0.5 **	NA
10	38.4	11.8	2915	-4.76 **	-18.17 *	106.61 **	2

[4] Mouse clicks taken to access the privacy policy from the home page.

A negative deviation value on the FGL score can be observed in Table 4 for all the privacy policies; this is a positive observation, as a lower FGL score means that the text is easier to comprehend. On the other hand, the word counts for all 10 privacy policies are higher than the known average. This is a negative observation, thus these values are coloured using orange. For the FRES score, only two privacy policies are more difficult to comprehend when compared to the average value of 40.32. For the Transparency or Ease of Access guideline, the majority of the websites, 60%, require only one click, and 30% of the websites require a total of two clicks to access the privacy policy from the website home page. One of the websites, website 9, did not have a hyperlink available to the privacy policy on the home page, the privacy policy was instead found by searching for it using a search engine.

6 Discussion and Recommendations

Not one of the 10 websites addressed all 14 website privacy policy guidelines as discussed in section 5. To address the shortcomings, recommendations are listed in Table .

Table 5. Recommendations for South African e-commerce website privacy policies

Shortcoming and Recommendation
Not meeting the holistic privacy policy guidelines None of the privacy policies reviewed met all the requirements of the 14 privacy policy guidelines that are part of the holistic privacy policy guidelines for websites. For this reason, it would be beneficial for the website owners to review their privacy policies with the proposed privacy policy guidelines in Appendix A.

Shortcoming and Recommendation
Inadequate data privacy The proposed guidelines are not a compliance review of POPIA but indicate that certain conditions of POPIA were not met. For example, the Data Subject Participation (Condition 8), which is linked to the privacy policy guideline *User Control*. The user should be able to control who accesses their data, request their data to be deleted, and control who shares their data [7], [49]. Detailed information on the *User Control* guideline was rarely noticed in the website privacy policies. It is highly recommended that this information be added in a clear and easy-to-understand way. As discussed in subsection 3.3 of this research, Amos et al. [30] also found that privacy policies lack transparency concerning third-party user details and technologies that track users. Subsection 3.3 also discusses that companies can provide security and control to their consumers by implementing privacy policies based on internet governance procedures [42].
Lengthy privacy policies All of the 10 privacy policies reviewed, exceeded the average word count of privacy policies as measured by [64]. Shortening the privacy policies can encourage users to read the policies, spreading better awareness of the content or privacy policies. Reinhardt et al. [31] mention the possible use of visual representations in online privacy policies; this can make the policies more attractive and reduce the amount of text used in the policy. An online privacy policy's visual and interactive interfaces can also be modified to increase user-friendliness, usability and reading willingness characteristics [35].
Comprehension and readability The privacy policies must be easy to understand; although the overall findings on the FRES score are positive, this is still a characteristic that can be improved further. For example, Micheti et al. [34] propose a comprehensive list of privacy policy guidelines that can be applied to policies to make them easier for teens and children to understand. Some of these guidelines focus on textual guidelines, such as avoiding double negatives, and others focus on structural and design approaches to privacy policies.

A future study could benefit from a larger sample and using a random selection technique for the websites rather than one based on popularity, as this could increase the diversity of the results. A limitation of the study is that the proposed guidelines do not represent a compliance review of POPIA and future work would benefit by developing and integrating POPIA-based website privacy policy compliance requirements with an independent expert panel review to further expand and improve the proposed guidelines.

7 Conclusion

A holistic set of privacy policy guidelines, mapped to POPIA conditions, was proposed based on a scoping literature review. This consists of 14 privacy policy guidelines, with 24 questions that website owners can use to aid in developing website privacy policy content. Using an embedded single-case study design, the proposed privacy policy guidelines were used to analyse South African B2C e-commerce website privacy policies in line with the guidelines. It was found that none of the website privacy policies fully addressed the proposed guidelines. The research provides recommendations to South African website owners to improve their website privacy policies. This will contribute to improving compliance with POPIA which, in turn, can also increase South African consumers' trust levels. Future research can further validate the proposed website privacy policy guidelines by incorporating a compliance perspective from POPIA and applying it in larger samples.

References

1. Revinova, S.: E-Commerce in BRICS: Similarities and Differences. International Journal of Economic Policy in Emerging Economies. 12, 377–389 (2019).
2. Kordić, N.: The extent of e-commerce presence in developing countries. In: Proceedings of the 1st International Scientific Conference - Sinteza 2014. pp. 313–317. Singidunum University, Belgrade, Serbia (2014). https://doi.org/10.15308/sinteza-2014-313-317.
3. Earp, J.B., Anton, A.I., Aiman-Smith, L., Stufflebeam, W.H.: Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Trans Eng Manag. 52, 227–237 (2005).
4. Protection of Personal Information, Act 4 of 2013, https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf%0A, last accessed 2022/05/22.
5. Netshakhuma, N.S.: Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). Global Knowledge, Memory and Communication. 69, 58–74 (2020).
6. Agrawal, R., Grosky, W.I., Fotouhi, F.: Ranking Privacy Policy. In: Proceedings of IEEE 23rd International Conference on Data Engineering Workshop. pp. 192–197. IEEE (2007). https://doi.org/10.1109/ICDEW.2007.4400991.
7. Javed, Y., Salehin, K.M., Shehab, M.: A Study of South Asian Websites on Privacy Compliance. IEEE Access. 8, 156067–156083 (2020). https://doi.org/10.1109/ACCESS.2020.3019334.
8. Tjhin, I., Vos, M., Munaganuri, S.: Privacy governance online: Privacy policy practices on New Zealand websites. Proceedings of Pacific Asia Conference on Information Systems, PACIS 2016. (2016).
9. Eckert, A., Milan, G.S., Roy, G., Bado, R.: Welcome back: Repurchase intention of Brazilian customers on e-commerce websites. Revista de Ciências da Administração. 23, 106–120 (2021).
10. B. Meinert, D., K. Peterson, D., R. Criswell Ii, J., D. Crossland, M.: Would Regulation of Web Site Privacy Policy Statements Increase Consumer Trust? Informing Science: The International Journal of an Emerging Transdiscipline. 9, 123–142 (2006). https://doi.org/10.28945/476.
11. Wu, K.-W., Huang, S.Y., Yen, D.C., Popova, I.: The effect of online privacy policy on consumer privacy concern and trust. Comput Human Behav. 28, 889–897 (2012).
12. Malapane, T.A.: A Risk Analysis of E-Commerce: A Case of South African Online Shopping Space. In: 2019 Systems and Information Engineering Design Symposium (SIEDS). pp. 1–6. IEEE (2019).
13. Anic, I.-D., Škare, V., Kursan Milaković, I.: The determinants and effects of online privacy concerns in the context of e-commerce. Electron Commer Res Appl. 36, 100868 (2019).
14. Staunton, C., Adams, R., Botes, M., Vries, J. de, Labuschaigne, M., Loots, G., Mahomed, S., Loideain, N.N., Olckers, A., Pepper, M.S., Pope, A., Ramsay, M.: Enabling the use of health data for research: Developing a POPIA code of conduct for research in South Africa. S Afr J Bioeth Law. 14, 33–36 (2021).
15. Aladeokin, A., Zavarsky, P., Memon, N.: Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. In: Proceedings of Twelfth International Conference on Digital Information Management (ICDIM). pp. 121–126. IEEE (2017).
16. Ki Bareh, C.: Assessment of the Privacy and Security Practices of the Indian Academic Websites. Library Philosophy and Practice. (2021).
17. Tesfay, W.B., Hofmann, P., Nakamura, T., Kiyomoto, S., Serna, J.: Privacyguide: Towards an implementation of the EU GDPR on internet privacy policy evaluation. IWSPA 2018 - Proceedings of the 4th ACM International Workshop on Security and Privacy Analytics, Co-located with CODASPY 2018. 2018-Janua, 15–21 (2018). https://doi.org/10.1145/3180445.3180447.
18. Steyn, L.J., Mawela, T.: A Trust-based e-Commerce Decision-making Model for South African Citizens. In: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists on - SAICSIT '16. pp. 1–9. ACM Press, New York, New York, USA (2016).
19. Mofokeng, T.E.: An empirical study stepping towards ethnographic research for e-commerce websites: A perspective of user-centred design. African Journal of Science, Technology, Innovation and Development. 0, 1–19 (2021). https://doi.org/10.1080/20421338.2021.1958987.
20. Hung, P.C.K., Cheng, V.S.Y.: Privacy. In: Encyclopedia of Database Systems. pp. 2136–2137. Springer US, Boston, MA (2009). https://doi.org/10.1007/978-0-387-39940-9_274.
21. Cappel, J.J., Shah, V., Verhulsdonck, G.: Perceptions of Online Privacy. Journal of Business and Educational Leadership. 10, 122–133 (2020).
22. Lockhat, R.: Social media and the Protection of Personal Information Act. Southern African Journal of Anaesthesia and Analgesia. 27, 69–72 (2021). https://doi.org/10.36303/SAJAA.2021.27.6.S1.2702.

23. Staunton, C., Tschigg, K., Sherman, G.: Data protection, data management, and data sharing: Stakeholder perspectives on the protection of personal health information in South Africa. PLoS One. 16, e0260341 (2021). https://doi.org/10.1371/journal.pone.0260341.
24. Jiang, Y., Syn, T.: Online Privacy Policy Disclosure: An Empirical Investigation. Journal of Computer Information Systems. 00, 1–18 (2022). https://doi.org/10.1080/08874417.2022.2095542.
25. Sindermann, C., Schmitt, H.S., Kargl, F., Herbert, C., Montag, C.: Online Privacy Literacy and Online Privacy Behavior – The Role of Crystallized Intelligence and Personality. Int J Hum Comput Interact. 37, 1455–1466 (2021). https://doi.org/10.1080/10447318.2021.1894799.
26. Brunotte, W., Chazette, L., Kohler, L., Klunder, J., Schneider, K.: What About My Privacy?Helping Users Understand Online Privacy Policies. In: Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering. pp. 56–65. ACM, New York, NY, USA (2022). https://doi.org/10.1145/3529320.3529327.
27. Kretschmer, M., Pennekamp, J., Wehrle, K.: Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. ACM Transactions on the Web. 15, 1–42 (2021).
28. Capistrano, E.P.S., Chen, J.V.: Information privacy policies: The effects of policy characteristics and online experience. Comput Stand Interfaces. 42, 24–31 (2015).
29. Steinfeld, N.: "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. Comput Human Behav. 55, 992–1000 (2016).
30. Amos, R., Acar, G., Lucherini, E., Kshirsagar, M., Narayanan, A., Mayer, J.: Privacy Policies over Time: Curation and Analysis of a Million-Document Dataset. In: Proceedings of the Web Conference 2021. pp. 2165–2176. ACM, New York, NY, USA (2021).
31. Reinhardt, D., Borchard, J., Hurtienne, J.: Visual interactive privacy policy: The beter choice? Proceedings of Conference on Human Factors in Computing Systems. (2021).
32. Kotal, A., Joshi, K.P., Joshi, A.: ViCLOUD: Measuring Vagueness in Cloud Service Privacy Policies and Terms of Services. In: Proceedings of IEEE 13th International Conference on Cloud Computing (CLOUD). pp. 71–79. IEEE (2020). https://doi.org/10.1109/CLOUD49709.2020.00023.
33. Proctor, R.W., Ali, M.A., Vu, K.-P.L.: Examining Usability of Web Privacy Policies. Int J Hum Comput Interact. 24, 307–328 (2008). https://doi.org/10.1080/10447310801937999.
34. Micheti, A., Burkell, J., Steeves, V.: Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand. Bull Sci Technol Soc. 30, 130–143 (2010)..
35. Ibdah, D., Lachtar, N., Raparthi, S.M., Bacha, A.: "Why Should I Read the Privacy Policy, I Just Need the Service": A Study on Attitudes and Perceptions Toward Privacy Policies. IEEE Access. 9, 166465–166487 (2021). https://doi.org/10.1109/ACCESS.2021.3130086.
36. Zaeem, R.N., Barber, K.S.: The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. ACM Trans Manag Inf Syst. 12, 1–20 (2021). https://doi.org/10.1145/3389685.
37. Lin, X., Liu, H., Li, Z., Xiong, G., Gou, G.: Privacy protection of China's top websites: A Multi-layer privacy measurement via network behaviours and privacy policies. Comput Secur. 114, 102606 (2022).
38. Prinsloo, P., Kaliisa, R.: Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. British Journal of Educational Technology. 53, 894–913 (2022).
39. Botha, J., Grobler, M.M., Hahn, J., Eloff, M.: A high-level comparison between the South African protection of personal information act and international data protection laws. Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017. 57–66 (2017).
40. Oki, O., Ngotshane, S.: Investigating the Effects of Covid-19 on Online Shopping Cybercrime in Buffalo City. In: Proceedings of 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). pp. 1–6. IEEE (2021).
41. Mutemwa, M., Mtsweni, J., Mkhonto, N.: Developing a cyber threat intelligence sharing platform for South African organisations. In: Proceedings of 2017 Conference on Information Communication Technology and Society (ICTAS). pp. 1–6. IEEE (2017).
42. van Ooijen, I., Vrabec, H.U.: Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. J Consum Policy (Dordr). 42, 91–107 (2019).
43. Lung, S.L., Wincentak, J., Gan, C., Kingsnorth, S., Provvidenza, C., McPherson, A.C.: A scoping review of suggested practices for healthcare providers when discussing sexuality with youth. Can J Hum Sex. 31, 143–160 (2022). https://doi.org/10.3138/cjhs.2021-0058.
44. Rumrill, P.D., Fitzgerald, S.M., Merchant, W.R.: Using scoping literature reviews as a means of understanding and interpreting existing literature. Work. 35, 399–404 (2010).
45. Zachary, M., Micah D. J., P., Cindy, S., Catalin, T., Alexa, M., Edoardo, A.: Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodol. 18, 1–7 (2018).

46. Page, M.J., Moher, D., McKenzie, J.E.: Introduction to PRISMA 2020 and implications for research synthesis methodologists. Res Synth Methods. 13, 156–163 (2022). https://doi.org/10.1002/jrsm.1535.
47. Asif, M., Javed, Y., Hussain, M.: Automated Analysis of Pakistani Websites' Compliance with GDPR and Pakistan Data Protection Act. In: Proceedings of International Conference on Frontiers of Information Technology (FIT). pp. 234–239. IEEE (2021). https://doi.org/10.1109/FIT53504.2021.00051.
48. Bufalieri, L., Morgia, M. La, Mei, A., Stefa, J.: GDPR: When the Right to Access Personal Data Becomes a Threat. In: Proceedings of 2020 IEEE International Conference on Web Services (ICWS). pp. 75–83. IEEE (2020). https://doi.org/10.1109/ICWS49710.2020.00017.
49. Chang, Y., Wong, S.F., Libaque-Saenz, C.F., Lee, H.: The role of privacy policy on consumers' perceived privacy. Gov Inf Q. 35, 445–459 (2018). https://doi.org/10.1016/j.giq.2018.04.002.
50. Coleti, T.A., Correa, P.L.P., Filgueiras, L.V.L., Morandini, M.: TR-Model. A Metadata Profile Application for Personal Data Transparency. IEEE Access. 8, 75184–75209 (2020). https://doi.org/10.1109/ACCESS.2020.2988566.
51. Fouad, I., Santos, C., Al Kassar, F., Bielova, N., Calzavara, S.: On Compliance of Cookie Purposes with the Purpose Specification Principle. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 326–333. IEEE (2020). https://doi.org/10.1109/EuroSPW51379.2020.00051.
52. Mamakou, X.J., Kardaras, D.K., Papathanassiou, E.A.: Evaluation of websites' compliance to legal and ethical guidelines: A fuzzy logic–based methodology. J Inf Sci. 44, 425–442 (2018). https://doi.org/10.1177/0165551517697610.
53. Nwaeze, A.C., Zavarsky, P., Ruhl, R.: Compliance evaluation of information privacy protection in e-government systems in Anglophone West Africa using ISO/IEC 29100:2011. In: Proceedings of Twelfth International Conference on Digital Information Management (ICDIM). pp. 98–102. IEEE (2017). https://doi.org/10.1109/ICDIM.2017.8244644.
54. Zaeem, R.N., German, R.L., Barber, K.S.: PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining. ACM Trans Internet Technol. 18, 1–18 (2018). https://doi.org/10.1145/3127519.
55. Nilmanat, K., Kurniawan, T.: The quest in case study research. Pac Rim Int J Nurs Res Thail. 25, 1–6 (2020).
56. Woodside, A.G., Wilson, E.J.: Case study research methods for theory building. Journal of Business & Industrial Marketing. 18, 493–508 (2003). https://doi.org/10.1108/08858620310492374.
57. Yin, R.K.: Case study research : design and methods. Sage Publications, Thousand Oaks, Calif. (2003).
58. Schoch, K., Burkholder, G., Cox, K., Crawford, L., Hitchcock, J.: Research design and methods : an applied guide for the scholar-practitioner. SAGE Publications, Inc., Thousand Oaks, California (2019).
59. Lenz, A.S.: Using Single-Case Research Designs to Demonstrate Evidence for Counseling Practices. Journal of Counseling & Development. 93, 387–393 (2015). https://doi.org/10.1002/jcad.12036.
60. Taherdoost, H.: Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. SSRN Electronic Journal. 5, 18–27 (2016). https://doi.org/10.2139/ssrn.3205035.
61. Seawright, J., Gerring, J.: Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Option. Polit Res Q. 61, 294–308 (2008). https://doi.org/10.1177/1065912907313077.
62. Jensen, C., Potts, C.: Privacy policies as decision-making tools: an evaluation of online privacy notices. In: Proceedings of the 2004 conference on Human factors in computing systems - CHI '04. pp. 471–478. ACM Press, New York, New York, USA (2004). https://doi.org/10.1145/985692.985752.
63. Proctor, R.W., Ali, M.A., Vu, K.-P.L.: Examining Usability of Web Privacy Policies. Int J Hum Comput Interact. 24, 307–328 (2008). https://doi.org/10.1080/10447310801937999.
64. Srinath, M., Wilson, S., Giles, C.L.: Privacy at Scale: Introducing the PrivaSeer Corpus of Web Privacy Policies. In: Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers). pp. 6829–6839. Association for Computational Linguistics, Stroudsburg, PA, USA (2021). https://doi.org/http://dx.doi.org/10.18653/v1/2021.acl-long.532.
65. Udayanga, V., Jayarajah, U., Colonne, S.D., Seneviratne, S.A.: Quality of the patient-oriented information on thyroid cancer in the internet. Health Policy Technol. 9, 302–307 (2020). https://doi.org/10.1016/j.hlpt.2020.03.007.

Appendix A: Website privacy policy guidelines

Website Privacy Policy Guidelines	**POPIA mapping**	**Description**	**Questions**
Accuracy of Data	Information Quality (Condition 5)	The information set out in the privacy policy must be up to date, and the terms discussed in the policy should be accurate and true [52].	Q1. Is the information defined in the privacy policy up to date (are there any timestamps showing when the policy was last updated)?
Assurances	Accountability (Condition 1)	Defines the third-party laws that govern how the responsible party of the website manages and processes data and ensures that the privacy policy is constructive [6], [49].	Q2. Are the third-party laws that govern how the responsible party of the website manages and processes the data made available (are any details given about POPIA or the Information Regulator of South Africa)?
Breach Notification	Security Safeguards (Condition 7)	This is the notification guarantee that the website provides to the data subject. If any form of data breach occurs, this breach must be communicated with the data subject. The breach will also be reported to the applicable authority [7], [47].	Q3. Will the data subject be notified if a breach of personal data occurs?
			Q4. Does the policy contain the steps and processes that will be followed if a breach occurs?
			Q5. Will the breach be reported to the appropriate authority?
Clarity of the Privacy Policy	Openness (Condition 6)	It must be easy to comprehend and not be long and tedious, which may discourage users from reading it [37], [51].	Q6. Is the policy easy to comprehend and not long and tedious? *The FRES and FGL scores can be calculated to determine if the policy is easy to comprehend. Readable.com can be used to determine the FRES score, FGL score and word count.*
Cross-border data transfer and Portability	Further Processing Limitation (Condition 4)	The user or data subject must be aware of any personal data or information transferred outside the original borders of consent [47], [50]	Q7. Are any details given on cross-border data transfer?
Data Collection Sources and Purpose	Processing limitation (Condition 2)	Includes the sources and purpose of collecting the data [47]. Only data that is essential for processing should be collected, and the collection volume should not exceed the privacy policy definitions [37].	Q8. Are the data collection sources and purposes defined?
			Q9. Is it defined that only the data that is essential for processing is collected and that the collection volume will not exceed the privacy policy definitions?
Data Processing and Consent	Processing limitation (Condition 2)	Encompasses the requirements and purpose for data processing. The data subject must provide consent for any data that will be processed, and the type of data to be processed should be made clear in the privacy policy [47], [53].	Q10. Is consent obtained from the data subject before any data is processed?
			Q11. Is the type of data that will be processed made clear in the privacy policy?
Data Retention	Purpose Specification (Condition 3)	Defines the data retention period of the processing body. The privacy policy should also provide details on when the data subject's personal data will be deleted or removed [37].	Q12. Is the data retention period by the processing body provided?
			Q13. Are details provided on when the data subject's data will be deleted or removed?
Data Security Measures	Security Safeguards (Condition 7)	The personal information and data of the user must be protected and secured by the data operator. Personal data must also be guarded and protected when transferred [52]. The data operator should provide assurances and steps taken to protect the integrity of the data [49].	Q14. Information and data of the user must be protected and secured by the data operator, are security measures in place to protect the data?
			Q15. Personal data must also be guarded and protected when transferred. The data operator should provide assurances and steps taken to protect the integrity of the data. Are these steps defined?
Disclosure of Privacy Policy	Openness (Condition 6)	It is vital for the privacy policy to be visible and openly available on the website accessed, informing the user of their rights [48].	Q16. Is the privacy policy openly available on the website?
Entity	Openness (Condition 6)	Provides information on the website, data operator and processor. In addition, the website should provide contact details on how the data subject can contact them [6].	Q17. Information about the website, data operator and processor must be provided in the privacy policy, is this information available?
			Q18. Does the website provide contact details for the data subject on how to contact them?
Transparency and Ease of Access	Openness (Condition 6)	The privacy policy should be uncomplicated to find on the website, and access to the privacy policy should not be complicated or misleading [37].	Q19 Is the privacy policy easily found on the website (access to the privacy policy should not be complicated or misleading)? *This can be calculated by counting the number of clicks it takes to reach the website privacy policy.*
Third-Party Data Users and Disclosure of Personal Data	Further Processing Limitation (Condition 4)	If data is being shared or distributed with a third-party company, the data subject should be alerted, and consent should be obtained [47]. The roles of each third-party data user must be clearly defined [50].	Q20. If data is being shared or distributed with a third-party company, the data subject should be alerted, and consent should be obtained, is this consent mentioned or discussed in the privacy policy?
			Q21. Are the roles of each third-party data user clearly defined?
User Control	Data subject participation (Condition 8)	The data subject must be able to control who accesses their data [49]. Additionally, it must be possible for data subjects to ask for their data to be deleted. Finally, the sharing and processing of their data should be controllable [7].	Q22. Can the data subject control who accesses their data?
			Q23. Is it possible for the data subject to ask for their data to be deleted?