A Comparative Study of Privacy Compliance Testing Tools

Ehsan Tawfig Madani Tawfig[1] Prof. Khaled Ahmed Ibrahim[2]
1 Faculty of Computer Sciences & Info. Technology Nile Valley University
2Faculty of Computer Sciences & Info. Technology Karary University
Corresponding Author:
Email: Ehsan@nilevalley.edu.sd

Abstract

Privacy compliance testing tools play a vital role in today's digital age. They help protect personal data, ensure compliance with laws and regulations, and reduce risks. This research compares eleven privacy compliance testing tools based on thirteen evaluation criteria. The results show that most of the tools support artificial intelligence technologies, which enhances their ability to analyze data and detect potential risks quickly and effectively. All tools are compliant with international standards and regulations, but do not directly support the Sudanese AntiCybercrime Law (2007). The analysis indicates a preference for comprehensive tools that offer integrated solutions, with the possibility of customization to meet the needs of the organization. It also emphasizes the importance of ease of use, multilingual support, high performance, and the ability to provide comprehensive reports. The research shows that most of the tools are not open source and require financial investment. The research reviews the different tools according to criteria such as speed of performance, release date, reporting support, scalability, and technical support, which helps in choosing the most suitable tool for organizations according to their specific needs.

Keywords: E-privacy, Privacy Compliance Testing Tools, Protecting Personal Data, Compliance with Laws and Regulations.

1. Introduction

In the digital age, the adoption of E-government services has become increasingly widespread, offering numerous benefits such as improved accessibility, efficiency, and transparency in public administration. However, the transition to digital platforms also brings significant concerns regarding the privacy of citizens' data. E-privacy, defined as the protection of personal information in electronic communications, is a critical aspect that governments must address to gain and maintain public trust. The importance of E-privacy in the context of egovernment cannot be overstated. As governments collect, store, and process vast amounts of personal data, ensuring the security and privacy of this information is paramount. Citizens need to feel confident that their data is protected from unauthorized access, misuse, and breaches.

As users become more aware of their rights to maintain the privacy of their data, laws and regulations related to privacy have become more stringent and complex. For example, the General Data Protection Regulation (GDPR) in the European Union in 2018 introduced a strict set of rules governing how personal data is collected, used, and stored. Similarly, the California Consumer Privacy Act (CCPA) provided a legal framework for data protection in the United States. This is where privacy compliance testing tools come into play. These tools help governments monitor and assess the extent to which their processes and procedures are in compliance with privacy-related legal regulations. These tools go beyond mere data analysis to provide deep insights that enable governments to make strategic decisions to protect citizen's data. Additionally, they identify security gaps and weaknesses in information systems, which helps in strengthening preventive measures and reducing the risk of breaches. As the use of these tools expands, they have become an integral part of government's compliance and governance strategies. Although there are many privacy compliance testing tools available in the market, their wide variations in features, performance, and effectiveness make choosing the right tool a complex task. These tools vary in their capabilities, from the ability to manage customer data to providing detailed compliance reports. Hence, the need for a comprehensive comparative study between these tools has become urgent. This study is not only essential to understand the differences between them, but it also provides government's with the knowledge to make informed decisions about investing in the tool that best meets their needs.

This paper aims to bridge the knowledge gap by providing a comprehensive analysis and detailed comparison of the leading tools in the field of privacy compliance testing. The tools will be analyzed based on a set of criteria, the most important of which are support for artificial intelligence, compliance with legal standards, ease of use, customizability, speed of performance, support for multiple languages, release date, comprehensiveness of reports, scalability, and technical support. Through this analysis, we hope to help government's choose the tool that best suits their requirements and regulatory needs.

The paper begins with a review of the available literature on compliance testing tools, pointing out the key concepts and recent trends in this field. This is followed by the research methodology, which explains how the tools were selected and the criteria used in the comparison. After that, a detailed analysis of the selected tools is provided, highlighting the strengths and weaknesses of each tool.

Finally, this article discusses the findings of this study by comparing privacy compliance tools with a focus on AI support, customizability, and multilingual capabilities to help governments and organizations choose the right tools to enhance their ability to meet future challenges in this area.

2. LITERATURE REVIEW

A. E-government services and privacy concerns

(Chakraborty, G S Prakasha, & C K Sripavithra, 2021) Investigate data-privacy anxiety among Indians, particularly during the COVID-19 pandemic. it employs an inductive qualitative exploratory approach with reflexive thematic analysis to analyze interviews of participants. The study identifies six themes and 26 sub-themes as determinants of data-privacy anxiety, highlighting systemic issues in knowledge dissemination and the paradox of learned helplessness and convenience preference. The study critiques current knowledge

dissemination methods for contributing to anxiety and argues for a critical pedagogy approach to educate the public on digital security. The paper suggests modifications in policies and documentation processes of online platforms and apps to reduce uncertainty and insecurity among users. It emphasizes the need for user-involving approaches and customized educational programs based on social locations to address data-privacy concerns effectively.

The research underscores the psychological impacts of data breaches, noting increased anxiety among participants due to information overload and inadequate digital knowledge. It calls for transparent, user-friendly policies and a multidisciplinary approach to studying media's complex role in society. Future research is encouraged to combine qualitative and quantitative methods to develop comprehensive solutions for data privacy and user behavior, ensuring safer digital usage for all age groups.

(Dhagarra, Mohit Goswami, & Gopal Kumar, 2020) Investigate the factors influencing patients' acceptance of technology in healthcare service delivery, focusing on trust and privacy concerns. The authors extend the Technology Acceptance Model (TAM) to include behavioral traits (trust and privacy concerns) and cognitive beliefs (perceived usefulness and perceived ease of use). They conducted a survey with 416 patients from primary health centers in New Delhi, India, and used structural equation modeling (SEM) to test their conceptual model. Key findings include: Trust significantly influences patients' behavioral intentions to use healthcare technology, as well as their perceptions of the technology's usefulness and ease of use. Privacy concerns negatively impact patients' perceived usefulness, ease of use, and behavioral intentions regarding healthcare technology. Both trust and privacy concerns are critical determinants in the acceptance of healthcare technology.

The study highlights that trust can reduce the perceived risks associated with technology use, thereby enhancing acceptance. Conversely, high privacy concerns can deter patients from adopting new technologies due to fears of data misuse. The research provides valuable insights for healthcare managers, emphasizing the need to build trust and address privacy concerns to facilitate technology adoption in healthcare services. Overall, this study underscores the importance of considering patients' behavioral and cognitive factors when implementing new healthcare technologies, offering a comprehensive framework for understanding technology acceptance in this context.

(Amini Mulia, Fatimah Azzahro, & Putu Wuri Handayani, 2020) Investigate the factors influencing online privacy concerns among e-commerce users, with a focus on gender differences. The research analyzes internal factors such as personal information control and trust, and external factors like social influence and perceived risks. Key findings include:

Women tend to have higher privacy concerns compared to men. Trust in e-commerce platforms significantly reduces privacy concerns. Social influence plays a more critical role in shaping privacy concerns among women. The study highlights the importance of personal information control in mitigating privacy concerns. The study uses surveys to collect data from e-commerce users. Data analysis involves statistical methods to compare gender differences in privacy concerns. Tailored strategies are needed to address gender-specific privacy concerns, especially for women. Increased awareness and control over personal information can help reduce privacy concerns. The study provides valuable insights for e-commerce businesses to improve user trust and privacy management practices, ultimately enhancing user satisfaction and engagement.

(Hyun Cho, Sae Yong Oh, Ho Gun Rou, & Gwang Yong Gim, 2019) Aim to identify factors influencing the continuous use of e-government services, particularly focusing on privacy and security concerns. A survey of 318 users was conducted, with 284 valid responses analyzed using SPSS and Smart PLS. The study investigated how quality factors (service quality, system quality, information quality) and risk factors (privacy, security) affect perceived ease of use and perceived usefulness. Results showed that service and information quality positively impacted perceived usefulness, while system quality did not. Both privacy and security factors significantly affected users' trust in e-government services. Trust, perceived usefulness, and user satisfaction were found to be interrelated, with user satisfaction positively influencing the intention to continuously use e-government services. Contrary to expectations, perceived ease of use did not impact

perceived usefulness. The study's findings provide insights for improving e-government service delivery and building user trust, especially in the context of the 4th Industrial Revolution, highlighting the importance of addressing privacy and security concerns to enhance user satisfaction and continuous use intention.
(Liu & Lemuria Carter, 2018) Investigate the impact of citizens' privacy concerns on the adoption of e-government services. As government agencies increasingly suffer from data breaches, public concerns about information privacy are heightened. The study is grounded in the Theory of Reasoned Action (TRA) and explores how Internet users' information privacy concerns (IUIPC) influence their trust in the Internet (TOI) and perceived risks, which subsequently affect their intention to adopt egovernment services. The study identifies three key dimensions of IUIPC: collection, control, and awareness. These dimensions influence trust in the Internet and perceived risks, which are crucial determinants of e-government adoption. The research model hypothesizes that increased privacy concerns decrease trust and increase perceived risks, thereby reducing the likelihood of adopting e-government services.
Empirical evidence from the United States is used to test the proposed research model. The study employs a survey method to collect data from e-government users, aiming to understand their privacy concerns, trust levels, and perceived risks. The findings are expected to fill the gap in the literature regarding the negative aspects of e-government adoption, focusing on privacy and trust issues. The results suggest that familiarity with e-government systems can mitigate privacy concerns and enhance trust. Familiarity allows users to have clear expectations based on previous interactions, which helps reduce perceived risks and increase the likelihood of adopting egovernment services. Overall, this study highlights the importance of addressing privacy concerns and building trust to encourage the adoption of e-government services. It provides valuable insights for policymakers and practitioners to develop strategies that enhance user trust and reduce privacy risks in the digital government landscape.
(Mutimukwe, Ella Kolkowska, & Åke Grönlund, 2017) Discuss the challenges related to privacy concerns and their impact on trust and adoption of e-government services in Rwanda, as a developing country. The study aims to understand how privacy concerns affect citizens' use of e-government services, and to provide recommendations for improving these services.
The study focuses on four main research questions: What concerns do Rwandan citizens have about information privacy?
What are their perceptions of the effectiveness of privacy practices?
To what extent do they trust how personal information is used in e-government services?
What are their intentions towards using these services?
To collect data, questionnaires were distributed to 700 individuals, and 540 questionnaires were used successfully with a response rate of 77%. The sample included diverse geographic locations in Rwanda to provide a comprehensive representation of the country. The questionnaire relied on a seven-point Likert scale to assess the extent to which respondents agreed with a set of statements related to privacy concerns, trust, and usage intentions. The results showed that Rwandan citizens have significant concerns about information privacy, with the majority of respondents agreeing with statements related to privacy concerns. Despite this, citizens have some confidence in the effectiveness of privacy practices, but additional measures are needed to reassure them about how their personal information is handled. The study indicates that there is a positive trend towards the use of e-government services in Rwanda, but privacy concerns must be addressed to enhance trust and increase adoption rates. The study recommends the need to provide effective privacy practices and clarify how users' personal information is processed and stored. In conclusion, this study contributes to providing an empirical database to help improve e-government services in developing countries, through better understanding citizens’ concerns and improving privacy and trust practices.

B. Privacy and information security in e-governance

(Anic, Vatroslav Škare, & Ivana Kursan Milaković, 2019)
Investigate the factors influencing online privacy concerns (OPC) and their impacts on consumer behavior. Key findings include:

- Online privacy concerns (OPC) are significantly influenced by the desire for control over personal information and perceptions of weak government privacy regulation.
- Demographics (such as age and gender) and previous negative experiences with privacy invasions play a lesser role in determining OPC.
- Higher OPC leads to behaviors such as fabricating personal information and being less willing to share information online.
- OPC negatively affects attitudes towards online shopping, which in turn affects actual online purchases.
- There is no direct relationship between OPC and online purchases; the effect is mediated by attitudes towards online shopping.

The study highlights the need for improved privacy regulations and measures that give consumers more control over their personal data.

(C. Pandya & Narendra J. Patel, 2017) Aim to explore and identify research gaps in the field of Information Security (InfoSec) within the domain of E-Governance. The study highlights the necessity for specialized research to address the unique security challenges posed by E-Governance, as opposed to those encountered in E-Commerce. The security needs for EGovernance are more stringent from E-Commerce due to the sensitive nature of the data involved, such as personal and medical records. While the technical aspects might be similar, the processes, strategies, and regulatory requirements differ significantly. Effective information security is crucial for the successful implementation of E-Governance. The study finds that vulnerabilities like cross-site scripting (XSS) and SQL injection are prevalent in E-Governance websites, affecting their security. The paper emphasizes that non-technical factors play a significant role in InfoSec risks. These factors include management practices, regulatory environments, and the overall approach to security by public sector entities. The study identifies a gap in the availability of a comprehensive InfoSec model tailored for the Indian E-Governance context. Such a model should integrate both technical and non-technical aspects to effectively manage security risks.

(Omoogun, Preetila Seeam, Visham Ramsurrun, Xavier Bellekens, & Amar Seeam, 2017) Emphasize that eHealth data must meet rigid requirements for security, confidentiality, availability, access traceability, control, and long-term preservation, especially in cloud computing environments. Current eHealth systems often lack robust security mechanisms, making them vulnerable to various attacks and data breaches. The authors note that most eHealth devices and systems transmit data over the internet without sufficient endto-end encryption, posing significant risks during data transfer. To address these challenges, the paper discusses the legislative implications of data breaches and the importance of service provider accountability. It suggests that eHealth service providers should ensure transparency, user trust, and policy compliance, and be responsible for the security and privacy of their platforms. The paper also underscores the need for legal guidelines to protect users and regulate hardware/service providers, ensuring the security of personal data. Finally, the authors provide several security and privacy recommendations to enhance future eHealth implementations. These include incorporating end-to-end encryption, improving device and data security, and ensuring that service providers are held accountable for breaches. The goal is to build user trust and enhance the security of eHealth technologies as they become increasingly prevalent in healthcare.

(G. Hassan & Othman O. Khalifa, 2016) Address the critical importance of securing e-government services, highlighting the sensitive nature of governmental information and the need for robust security frameworks. It emphasizes the potential for egovernment to transform interactions between government entities and their stakeholders, including citizens and businesses. However, this transformation comes with significant security challenges, such as unauthorized access, malicious damage, data interception, and various cyber threats. The study proposes a framework for securing e-government services, combining multiple defense strategies to create a more resilient system. These strategies include defining security requirements, developing security policies, building a secure infrastructure, and conducting ongoing risk assessments and evaluations. The framework is designed to enhance trust between citizens and government, which is essential for the widespread adoption of e-government services. In conclusion, the research underscores the

necessity of integrating advanced security measures into e-government services to protect sensitive information, build trust, and encourage citizen engagement. It calls for a comprehensive approach that combines technical solutions with strategic policy-making to address the multifaceted nature of egovernment security challenges.

(SADKI & Hanan EL BAKKALI, 2014) Outline the advantages of EHRs, such as improved healthcare quality and reduced costs, while also noting the new security and privacy threats that arise from sharing patient data. The paper suggests that privacy must remain a fundamental right and should be personally controlled, regardless of the domain or context. several privacy-preserving approaches have been proposed, most of which focus on protecting private data using cryptographic, access control or anonymitization techniques. Thus, the patient becomes a passive actor regarding the disclosure of his personal information. The comparative study within the paper shows that recent research is beginning to consider patient preferences, particularly in the healthcare sector. The authors argue that patient trust in healthcare providers is crucial and can be increased by ensuring that sensitive information is kept private and secure. In summary, the paper advocates for a shift from third-party control to patient-controlled privacy in managing electronic health records, emphasizing the need for standards and regulations to support this shift.

C. Privacy compliance tools

(Martínez-Navalón, María Fernández-Fernández, & Fernanda Pedrosa Alberto, 2023) Examine the influence of privacy, ease of use, and trust on digital banking usage among Spanish and Portuguese students. It also investigates if nationality affects these variables. Data were collected through an online questionnaire and analyzed using PLS software. Key findings include: Privacy positively influences both trust and perceived ease of use. Higher perceived ease of use leads to greater consumer trust. No significant difference was found between nationalities regarding trust, privacy, and ease of use. Privacy and ease of use are crucial for building trust in digital banking. The study contributes to understanding the factors influencing digital banking adoption and highlights the importance of privacy and ease of use in enhancing consumer trust.

(Klinger, E, Wiesmaier, A, & Heinemann, A, 2022) Conducted a comprehensive comparison of privacy compliance tools, focusing on citizens' rights and SMEs' needs in implementing the requirements of the General Data Protection Regulation (GDPR). The paper reviews tools available to help individuals exercise their rights under the regulation, such as "Mine" and "DeleteMe" for searching accounts and deleting data, as well as consent management tools such as "PrivacyBee" and "SuperAgent," and data analytics tools such as "TransparencyVis." SMEs face challenges in complying with the regulation due to lack of resources and technical expertise. The paper compares tools available to these companies, such as "OneTrust," "Securiti.ai," "Osano," "Transcend," and "DataGrail." The comparison focuses on several criteria, most notably multilingual support, AI support, privacy compliance, customization and flexibility, ease of use, cost, performance and reporting, open source, and technical support. In the privacy compliance software market, tools like OneTrust, AvePoint, TrustArc, and IBM stand out by offering integrated compliance and risk management solutions. OneTrust offers flexible compliance management and multilingual support but can be expensive for small businesses. AvePoint focuses on data protection and reporting, with an easy-to-use interface. TrustArc supports global compliance and provides integrated reporting, but can take time to adapt to the system. IBM offers advanced AI-powered solutions, but they require high technical resources and cost (Department, 2024).

(Hasbullah & Wan Abdul Rahim Wan Mohd Isa, 2011) Aim to explore the adoption of privacy policies among Malaysian egovernment websites and to conceptualize an e-privacy assessment framework. Conducted by Nor Asiakin Hasbullah and colleagues, the research addresses the significance of privacy protection for sensitive information on these websites, especially in light of the Personal Data Protection Act 2009. The study examines the current level of awareness and implementation of privacy policies on federal and state government websites. Using a sample of 154 websites, the researchers evaluated the presence of privacy policy statements, notices, and links, based on indicators from previous studies by Jamal, Maier, and Sunder (2002). The findings reveal a mixed reality: while federal government websites largely include

privacy policies, state government websites show a lower adoption rate. The study highlights the need for standard privacy policy guidelines in Malaysia, noting the absence of a unified national standard. It underscores the importance of improved data protection and transparency to build trust between government agencies and citizens. The researchers suggest that establishing privacy policy standards through an eprivacy framework could enhance privacy protection across egovernment platforms. Concluding, the study emphasizes the necessity for further longitudinal research post-enforcement of the Personal Data Protection Act, development of automated tools for detecting invisible information gathering, and the creation of HCI research instruments to measure privacy adoption effectively.

3.RESEARCH METHODOLOGY

This study aims to conduct a comprehensive comparison between privacy compliance testing tools using a set of multiple criteria, to help determine the most appropriate tool for use by government and private institutions in protecting data privacy. A rigorous systematic approach was followed to select and evaluate the tools, ensuring the comprehensiveness and accuracy of the analysis.

Data collection and analysis methods: Data was collected using a variety of methods including reviewing the official documents of the tools, reviewing specialized reports and articles, and comparing the tools on reliable websites. In addition, user experiences and reviews provided by different platforms were analyzed. Through this analysis, the study aims to provide a balanced and accurate view of the advantages and disadvantages of the tools, helping governments and institutions choose the most appropriate tool for their requirements and needs.

A. CRITERIA FOR SELECTING PRIVACY COMPLIANCE TESTING TOOLS IN THE STUDY

The selection process of the tools was based on several key criteria aimed at evaluating the tools' efficiency and compatibility with the increasing privacy requirements of the digital age. These criteria included:

i. The tool's support for testing compliance with privacy requirements. ii. The comprehensiveness of the reports generated by the tool and its ability to provide detailed insights into compliance. iii. The availability of technical and functional support for the tool to users.

After reviewing 31 proposed tools from previous studies and specialized sources in electronic privacy, the researchers selected 11 tools that had the best characteristics based on the mentioned criteria. The aim of this selection is to provide a balanced analysis and comprehensive comparison that helps organizations make the best decision when choosing a privacy compliance testing tool. Below is a brief overview of the selected tools, arranged alphabetically, to identify their advantages and disadvantages in order to facilitate comparison between them.

[1] 2B Advice

2B Advice is an advanced privacy compliance management solution that provides a suite of tools to help organizations comply with privacy regulations such as GDPR and CCPA. It features advanced data analytics capabilities and provides detailed compliance reporting. It was selected because it focuses on providing comprehensive and integrated solutions that support organizations at various stages of data management and compliance.

[2] AvePoint Privacy Impact Assessment (PIA)

AvePoint PIA focuses on assessing the privacy impact and analyzing potential risks related to sensitive data. It provides comprehensive analytical reports that help organizations improve their security policies and comply with various laws. It was selected for its efficiency in providing accurate privacy assessment solutions and its ease of use in different environments.

[3] BigID

BigID relies on artificial intelligence and machine learning to identify and classify sensitive data within organizations. It provides advanced capabilities in predictive analytics and detailed reporting. It was selected because of its ability to support compliance with global privacy laws and help organizations identify and protect their data effectively.

[4] IBM OpenPages Data Privacy Management

IBM OpenPages offers a comprehensive privacy compliance management solution, with a suite of tools that enable risk assessment and efficient management of sensitive data. It features broad support for global privacy standards and the ability to integrate with various enterprise systems. It was chosen for its strong reputation and ability to deliver customized, advanced solutions.

[5] OneTrust PreferenceChoice

OneTrust PreferenceChoice provides user preference management capabilities and compliance with privacy laws such as GDPR and CCPA. It features an easy-to-use interface and multilingual support. It was chosen for its extensive customization capabilities that enable organizations to effectively manage privacy preferences.

[6] Securiti.ai

Securiti.ai uses artificial intelligence and machine learning technologies to protect data and ensure compliance with privacy laws. It features advanced analytics and reporting capabilities, helping organizations discover vulnerabilities and improve privacy policies. It was chosen for its technological sophistication and comprehensive support for various standards.

[7] TrustArc

TrustArc provides a comprehensive platform for managing compliance and data protection, allowing organizations to analyze and update privacy policies on a continuous basis. It offers integrated reporting and supports multiple languages, making it suitable for global use. It was chosen because it provides integrated solutions for organizations of all sizes.

[8] Crownpeak

Crownpeak is a comprehensive privacy compliance management tool with a focus on user experience and customizable interfaces. It supports global compliance standards and provides detailed reporting. It was chosen because it provides flexible solutions that help organizations meet diverse privacy requirements.

[9] DataPrivacyManager

DataPrivacyManager is a prominent privacy management tool, providing comprehensive risk assessment and compliance solutions. It offers advanced reporting and analysis capabilities, and supports global standards. It was chosen because it offers a good balance between efficiency and cost, making it suitable for various organizations.

[10] Ethical Data

Ethical Data focuses on promoting compliance with global privacy standards through advanced assessment and analysis tools. It provides innovative solutions for assessing privacy policies and procedures. It was chosen because it helps organizations comply with laws with the least possible cost and effort.

[11] Protiviti

Protiviti is a comprehensive tool that offers compliance and privacy management solutions combined with technical and support capabilities. It supports multiple languages and is customizable to meet the needs of different organizations. It was selected for its ability to meet the requirements of large and complex organizations.

All of these tools are aligned with the research objectives of providing an accurate and comprehensive analysis of the different tools on the market, helping governments and organizations make informed decisions about choosing the most appropriate compliance tool for their needs.

B. JUSTIFICATION FOR THE SELECTION OF CRITERIA FOR COMPARISON

These criteria have been carefully selected to ensure a comprehensive and balanced analysis of privacy compliance testing tools, so that governments and organizations can choose the tool that best suits their needs and regulatory requirements. These criteria allow for a careful comparison of tools based on technical, functional, legal, and economic aspects, supporting the primary goal of the research to provide a

comprehensive analysis that helps organizations make informed decisions based on a careful evaluation of the available tools to choose the most appropriate tool according to each organization's needs and requirements.

[1] AI Support

AI support is one of the essential criteria because it enhances the tool's ability to analyze large amounts of data quickly and accurately, predict potential risks, and detect potential privacy violations. AI helps organizations reduce the costs and time required to assess compliance through automation and improve the accuracy of analysis, which is in line with the research objectives of identifying the most advanced and efficient tools.

[2] Compliance with Standards and Regulations

This criterion represents the basic ability of the tool to ensure compliance with various global laws and standards such as GDPR and CCPA. Compliance with legal standards is essential for any organization to maintain its reputation and avoid legal penalties. Therefore, this criterion is essential for assessing the tool's ability to meet various regulatory requirements, which achieves one of the research objectives in ensuring that organizations comply with laws.

[3] Specialized or Comprehensive

This criterion deter mines whether a tool is specialized in a specific aspect of privacy compliance or comprehensive, covering all aspects related to compliance. Specialized tools focus on specific functions such as managing data access requests or detecting vulnerabilities, which may provide greater efficiency in those specific areas. Comprehensive tools, on the other hand, provide a full suite of features, such as compliance management, privacy impact assessments, and risk analysis, making them a suitable option for organizations seeking an integrated solution that covers all compliance needs. The research aims to evaluate both types of tools to determine which offers the best value based on the organization's needs, and therefore, this criterion includes comparing tools according to their coverage and core functionality.

[4] Customizability

This criterion reflects the tool's ability to adapt to the needs of each organization according to its specific requirements. Customizable tools enable organizations to modify settings, reports, and procedures to suit their specific environment, enhancing the effectiveness and usability of the tool. This criterion helps meet the research objectives by identifying tools that provide sufficient flexibility for diverse use.

[5] Ease of Use

This criterion is essential to assess how easy it is for users to use a tool without requiring extensive training. Compliance tools that are easy to use increase the efficiency of the process and reduce the likelihood of human error, which is in line with the research goal of identifying tools that provide a convenient and effective user experience.

[6] Free

Indicates the extent to which the tool is available for free or at low cost. Free or low-cost compliance tools help thirdcountry governments or small and medium-sized enterprises comply with legal standards without incurring significant financial burdens, which supports the research goal of finding options that suit different types of organizations.

[7] Multilingual Support

Multilingual support is a key standard for global organizations that handle data from users in multiple countries. Compliance tools provide multilingual support that enhances users' understanding of compliance requirements and facilitates use in diverse environments, helping to achieve the research goal of identifying appropriate tools for different markets.

[8] Open Source

This standard reflects transparency in the development of the tool by making the source code available to the technical community, which enhances trust and credibility in it. Open source tools provide

governments and organizations with the ability to customize the tool according to their specific needs, and adapt it to local compliance requirements without restrictions. They also contribute to enhancing digital security by allowing independent reviews of the software code, and discovering any vulnerabilities or flaws faster, making them a flexible and sustainable option for many organizations.

[9] Performance Speed

This criterion refers to the tool's ability to process data and perform compliance tests quickly. Fast compliance tools help organizations detect and remediate potential violations faster, reducing risk. This criterion supports the research objectives by identifying the most effective and efficient tools.

[10] Release Date

This criterion is important because it reflects how long the tool has been in the software market and its ability to adapt to the ever-changing privacy laws and standards, helping users assess the maturity and sophistication of the tool.

Older tools may offer more comprehensive documentation and strong community support, while newer tools incorporate the latest technologies and innovative approaches.

[11] Report Support

This criterion refers to the tool's ability to produce comprehensive and accurate reports that show the status of compliance and identify areas for improvement. Compliance tools that provide clear and detailed reports help organizations improve their security policies and procedures. This criterion supports the research objectives by providing accurate and reliable information to organizations.

[12] Scalability

This criterion reflects the tool's ability to adapt to the volume of data and future growth of the organization. Scalable compliance tools allow large and growing organizations to continue using the same tool without the need for major changes. This criterion supports the research objectives by identifying tools that can be used flexibly in different environments.

[13] Technical Support

Refers to the availability of technical support to users, which is an important criterion to ensure that the tool continues to operate efficiently and that any technical issues that may arise are addressed. Compliance tools that provide reliable technical support enhance user confidence and make their use safer, which is in line with the research objectives of providing recommendations for tools that provide strong user support.

ID	Name Of the Tool	AI Support	Compliance with Standards & Regulations	Comprehensive or Specialized	Customizability	Ease of Use	Free	Multilingual Support	Open Source	Performance Speed	Release Date	comprehensive reports	Scalability	Technical Support
1	2B Advice	F	T	Specialize.	F	T	F	T	F	T	2003	T	T	T
2	AvePoint	F	T	Compreh.	T	T	F	T	F	T	2001	T	T	T
3	BigID	T	T	Compreh.	T	T	F	T	F	T	2016	T	T	T
4	IBM OpenPages Data Privacy Management	T	T	Compreh.	T	T	F	T	F	T	2010	T	T	T
5	OneTrust	T	T	Compreh.	T	T	F	T	F	T	2016	T	T	T
6	Securiti.ai	T	T	Compreh.	T	T	F	T	F	T	2019	T	T	T
7	TrustArc	T	T	Compreh.	T	T	F	T	F	T	1997	T	T	T
8	Crownpeak	F	T	Specialize.	T	T	F	T	F	T	2001	T	T	T
9	DataPrivacyManager	F	T	Specialize.	T	T	F	T	F	T	2018	T	T	T
10	Ethical Data	T	T	Compreh.	F	F	T	F	F	F	2022	T	T	T
11	Protiviti	T	T	Compreh.	F	F	F	T	F	F	2002	F	F	T

Table No (1) Comparison of Privacy Compliance Testing Tools

4. ANALYSIS OF A COMPARISON TABLE OF PRIVACY COMPLIANCE TESTING TOOLS

After analyzing Table No. (1), which included a comparison of 11 tools for testing privacy compliance according to 13 evaluation criteria, the researchers reached the following conclusions:

[1] AI Support Analysis

The data shows that the majority of tools (7 out of 11) support AI technologies, which enhances their ability to analyze data, quickly and effectively detect potential risks, and improve compliance with standards. This highlights that organizations tend to favor tools that leverage advanced technologies such as AI to ensure a higher level of accuracy and speed in compliance processes.

BigID and Securiti.ai offer excellent support for AI and machine learning, using AI extensively for compliance management, data analysis, classification, and risk identification. IBM OpenPages Data Privacy Management, OneTrust PreferenceChoice, and TrustArc offer moderate AI support for some tools and functions, but not comprehensively. Ethical Data and Protiviti offer poor support, relying on traditional analytics techniques with limited use of AI. The tools that do not support AI are: 2B Advice, AvePoint Privacy Impact Assessment (PIA), Crownpeak, and DataPrivacyManager.

[2] Compliance with Standards and Regulations Analysis

The fact that all the tools in the table comply with international standards and regulations indicates that compliance is a non-negotiable factor when choosing a compliance testing tool. This demonstrates that privacy compliance tools must provide strong compliance with international laws and standards to ensure trust and credibility.

The Sudanese Anti-Cybercrime Law (2007) is directly relevant to data protection and online privacy in Sudan, as it aims to combat cybercrimes, including privacy violations, data theft, and unauthorized access to personal information. Although the law does not include detailed regulations as comprehensive data protection laws such as the General Data Protection Regulation (GDPR), it provides a general framework for protecting data from illegal activities of Sudanese citizens. All of the above tools do not directly support compliance with the Sudanese Anti-Cybercrime Law (2007). Each tool should be customized to ensure its compliance with the specific requirements of Sudanese law by reviewing policies and implementing additional measures if necessary.

[3] Comprehensive vs. Specialized

The data shows that 8 of the tools are considered comprehensive while 3 are classified as specialized. This indicates a general preference for comprehensive tools that offer integrated solutions that cover most aspects of privacy compliance. Comprehensive tools give organizations greater flexibility and avoid the need to use multiple tools to address different aspects of compliance.

BigID and Securiti.ai provide excellent support for comprehensiveness, covering a wide range of functions including data discovery, classification, automated compliance, risk assessment, individual rights management and data requests.

IBM OpenPages Data Privacy Management, OneTrust PreferenceChoice and TrustArc provide moderate support (somewhat comprehensive) as they offer a range of features but focus more on managing users' privacy preferences and compliance rather than providing complete solutions.

AvePoint Privacy Impact Assessment (PIA), Ethical Data and Protiviti provide weak support for comprehensiveness (partially comprehensive) as they offer a limited set of features focused on compliance assessment and data analysis, but are not comprehensive in all aspects. The following tools are (specialized) 2B Advice, Crownpeak, and DataPrivacyManager as they focus

more on specific functions in managing compliance in depth without being comprehensive in their functions.

[4] Customizability Analysis

8 out of 11 tools offer customization capabilities, reflecting that the ability to customize the tool to meet the specific needs of the organization is a vital requirement. This can be explained by the fact that organizations have different needs and requirements depending on their size and scope of work. The following tools BigID, OneTrust PreferenceChoice, and TrustArc provide excellent support for the customizability criterion, allowing for multiple settings to meet different needs.

The tools AvePoint Privacy Impact Assessment (PIA), Securiti.ai, and Crownpeak provide moderate support for the customizability criterion, offering flexible customization options but with limited capabilities compared to the tools in the first group.

The tools IBM OpenPages Data Privacy Management and DataPrivacyManager provide weak and limited support for the customizability criterion with a low level of customization that meets only specific needs. The following tools 2B Advice, Ethical Data, and Protiviti do not provide support for the customizability criterion, as they rely primarily on the default tool architecture presets rather than allowing them to be tailored to the user's needs.

[5] Ease of Use Analysis

9 out of 10 tools provide easy-to-use interfaces, reflecting the importance of providing a comfortable user experience to ensure the tool is adopted and used efficiently. Governments and organizations are looking for tools that can be used without the need for extensive training, which reduces operational costs.

The following tools (OneTrust PreferenceChoice and TrustArc) provide excellent support for the ease of use standard, as they provide easy and intuitive user interfaces, with clear guidance and built-in help for users.

The following tools (AvePoint, Securiti.ai, BigID, Crownpeak, and DataPrivacyManager) provide moderate support for the ease of use standard, as they provide organized user interfaces, but can be a bit complex for new users who need some time to get used to, as they require some technical expertise to understand all the capabilities and features available.

The following tools (IBM OpenPages Data Privacy Management and 2B Advice) provide weak support for the ease of use standard, as they provide a somewhat complex interface, which makes it difficult for new or non-expert users to use. The following tools (Ethical Data and Protiviti) do not meet the usability standard, as they lack an intuitive user interface and user-friendly design, making them unpreferable for users looking for quick and easy solutions.

[6] Free Tool Availability Analysis

The fact that most of the tools are not free (10 out of 11) suggests that good compliance tools often require financial investment from governments and organizations. This also reflects that providing sophisticated and comprehensive solutions requires financial support to ensure that the tool is continually developed and updated.

Ethical Data is completely free to use, making it a preferred option for organizations on a budget.

The following tools (OneTrust PreferenceChoice, Securiti.ai, and TrustArc) offer free trials for a limited period, with access to specific features, but require a paid subscription to take advantage of the full capabilities. The following tools (AvePoint, DataPrivacyManager, BigID, and IBM OpenPages Data Privacy Management) offer a limited trial period with very limited functionality, making them not a good option for those looking for longterm free solutions.

The following tools (2B Advice, Crownpeak, and Protiviti) do not offer any free or trial options, and require a paid subscription.

[7] Multilingual Support Analysis

Multilingual support is essential for tools seeking to enter global markets (10 out of 11 tools support this standard to varying degrees).

AvePoint, TrustArc, and OneTrust PreferenceChoice provide good support for multilingual support, including Arabic.

Securiti.ai, BigID, and IBM OpenPages Data Privacy Management provide moderate support for multilingual support, including Arabic, with some features limited. 2B Advice, Crownpeak, DataPrivacyManager, and Protiviti provide limited and weak support for multilingual support, and Arabic may not be well supported.

Ethical Data does not provide support for multilingual support.

[8] Open Source Analysis

The lack of open source tools suggests that privacy compliance tools tend to be proprietary, perhaps to protect their trade secrets and proprietary technologies. It may also be interpreted that proprietary tools provide more technical support and better security updates, which organizations consider necessary to protect their sensitive data. None of the tools on the list can be classified as open source. BigID offers some components open source and supports some integrations with open source tools, but it is not a fully open source tool. While Securiti.ai uses some open source technologies internally, it does not provide direct support for the Open Source standard.

[9] Performance Speed Analysis

Most tools have high performance speed (9 out of 11), reflecting the importance of this criterion in ensuring that the tool can handle large amounts of data and quickly comply with changing requirements. Performance speed is critical in environments that require rapid response to legal changes and potential risks.

These tools (BigID, Securiti.ai, TrustArc) provide excellent support for the Performance Speed criterion While these tools (AvePoint, OneTrust PreferenceChoice, IBM OpenPages Data Privacy Management) provide moderate support for the Performance Speed criterion as they are slower than the other tools when it comes to processing big data.

While these tools (2B Advice, Crownpeak, DataPrivacyManager) provide weak support for the Performance Speed criterion as these tools do not rely on AI and machine learning technologies.

These tools (Ethical Data and Protiviti) do not provide support for the Performance Speed criterion

As they do not focus heavily on performance speed as a primary criterion, they may be slow to process data or perform compliance tasks.

[10] Release Date Analysis

Tools released between 1997 and 2022 show a balance between older tools that have long experience and are constantly updated, such as TrustArc (1997), and newer tools that may incorporate new technologies and methodologies, such as Ethical Data (2022). Newer tools may have an advantage in supporting the latest technologies, while older tools may be more mature and reliable.

When ranking tools by release date, consider the most recent and regular updates to the tool.

The following tools (Securiti.ai, BigID, OneTrust PreferenceChoice) are relatively new tools but receive regular updates to add new features and improve performance.

While these tools (TrustArc, AvePoint, IBM OpenPages Data Privacy Management) offer moderate support for the Release Date criterion, they are not entirely new, but they receive regular updates to ensure compliance with modern regulations and changing requirements. While these tools (2B Advice, DataPrivacyManager, Crownpeak) provide poor support for the Release Date standard, as they are effective, they do not receive frequent enough updates to keep up with

the rapid developments in the compliance field. While these tools (Ethical Data and Protiviti) do not provide support for this standard, as they have not performed frequent or regular updates.

[11] Comprehensive Report Support Analysis

Most tools (10 out of 11) provide comprehensive reporting support, underscoring the importance of providing robust and comprehensive reporting tools for organizations to continually assess their compliance status and make decisions based on accurate data.

To rank privacy compliance testing tools according to the Comprehensive Report Support Analysis criterion, we need to consider each tool's ability to provide detailed and comprehensive privacy compliance reporting, including the ability to customize reports, analyze data, and provide clear and accurate information.

The following tools (BigID, TrustArc, Securiti.ai, and OneTrust PreferenceChoice) provide excellent support for comprehensive report analysis, with advanced features for customizing reports and analyzing data.

The following tools (AvePoint, IBM OpenPages Data Privacy Management, and DataPrivacyManager) provide good support for this criterion but may be limited in customizing in-depth reports or providing multidimensional analytics.

The following tools (2B Advice, Crownpeak, and Ethical Data) provide poor reporting support, as they do not provide the comprehensive or customized reports required to achieve excellent support for this criterion. While Protiviti does not offer any direct support in this context as it focuses on consulting services, it does not have specific tools or comprehensive reports ready for analysis and support.

[12] Scalability Analysis

Most tools (10 out of 11) provide comprehensive support for the scalability criterion, indicating the importance of compliance tools being flexible and adaptable as an organization grows and its needs increase. To rank privacy compliance testing tools according to the scalability analysis criterion, we look at each tool's ability to adapt and grow as data volumes, user counts, and complexity of operations or compliance across different geographies expand.

These tools (BigID, Securiti.ai, TrustArc, and IBM OpenPages Data Privacy Management) provide excellent support for the scalability analysis criterion, allowing organizations of all sizes to efficiently handle and analyze large amounts of data, allowing for easy scaling.

The following tools (OneTrust PreferenceChoice, DataPrivacyManager, and AvePoint) provide moderate support for the scalability analysis criterion, providing a good level of scalability, but may require additional customization to meet the needs of very large organizations. While these tools (Crownpeak, 2B Advice, and Ethical Data) offer poor support for Scalability Analysis, they offer limited scalability when dealing with larger or more complex organizations. Protiviti does not offer support for Scalability Analysis.

[13] Technical Support Analysis

The technical support available for all tools reflects that the tool should be backed by robust support services to ensure business continuity and quickly resolve issues that organizations may encounter while using the tool.

The following tools (BigID, TrustArc, IBM OpenPages Data Privacy Management, and Securiti.ai) provide excellent Technical Support, which includes dedicated support across multiple channels 24/7, a comprehensive knowledge base, and comprehensive customer guidance to ensure compliance.

The following tools (OneTrust PreferenceChoice, AvePoint, and Crownpeak) provide moderate Technical Support, providing good technical support, with customer support available across multiple channels, but it may not be available 24/7.

The following tools (DataPrivacyManager, 2B Advice, Ethical Data, and Protiviti) provide poor Technical Support, providing a limited level of technical support, which may be available

via email and chat only, with a lack of comprehensive resources or 24/7 support. Comparing privacy compliance testing tools makes it easier for researchers and developers to choose the right tool for them by showing how some tools excel at certain criteria, while others fall short. This helps governments and organizations understand the relative advantages and disadvantages of each tool, so they can make a more informed decision based on their specific needs.

5. CONCLUSION

The researchers reached several main conclusions through analyzing the comparison table. First, organizations prefer tools that rely on artificial intelligence technologies to improve the accuracy and speed of operations. Second, compliance with international standards is a prerequisite for selecting tools, while tools need to be customized to support local laws such as the Sudanese Anti-Cybercrime Law (2007). Third, comprehensive tools that provide integrated solutions are preferred over specialized tools, reflecting the ability to customize and expand, and meet the needs of different organizations. Fourth, ease of use and multi-language support are critical elements for tool adoption. Finally, the results indicate that non-open source tools provide better technical support and security updates, but require financial investment by organizations. This analysis helps governments and organizations make informed decisions based on the advantages and disadvantages of each tool according to their specific needs.

References

[1] Amini Mulia, R., Fatimah Azzahro, & Putu Wuri Handayani. (2020). Analysis of Internal and External Factors Affecting Online Privacy Concern in Ecommerce: Comparative Study by Gender. *International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 186193). Depok, Indonesia: IEEE.

[2] Anic, I.-D., Vatroslav Škare, & Ivana Kursan Milaković. (2019). The determinants and effects of online privacy concerns in the context of ecommerce. *Electronic Commerce Research and Applications*, 111.

[3] Boritz, J. E., & Won Gyun No. (2011). E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery. *JOURNAL OF INFORMATION SYSTEMS*, 8-45.

[4] C. Pandya, D., & Narendra J. Patel. (2017). Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 3-8.

[5] Chakraborty, R., G S Prakasha, & C K Sripavithra. (2021). Factors Affecting Data-Privacy Protection and Promotion of Safe Digital Usage. *Advanced in Information Security Management and Applications*, (pp. 49-59). Stavropol, Krasnoyarsk, Russia.

[6] Department, S. (2024 , August 26). *Data Privacy Software Market*. Retrieved from fortunebusinessinsights: https://www.fortunebusinessinsights.com/dataprivacy-software-market-105420

[7] Dhagarra, D., Mohit Goswami, & Gopal Kumar. (2020). Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare: An Indian Perspective. *International Journal of Medical Informatics*, 2-13.

[8] G. Hassan, R., & Othman O. Khalifa. (2016). EGovernment - an Information Security Perspective. *International Journal of Computer Trends and Technology (IJCTT)*, 1-9.

[9] Hasbullah, N. A., & Wan Abdul Rahim Wan Mohd Isa. (2011). Investigating the Privacy Policy Adoption among Malaysia E-Government Websites: Towards Conceptualizing the E-Privacy Assessment Framework. *International Journal on Advanced Science Engineering and Information Technology*, 311-317.

[10] Hyun Cho, S., Sae Yong Oh, Ho Gun Rou, & Gwang Yong Gim. (2019). A Study on The Factors Affecting The Continuous Use of E-Government Services - Focused on Privacy and Security Concerns -. *IEEE Computer Society*, 351-361.

[11] Kanaan, A., Ahmad AL-Hawamleh, Anas Abulfaraj, Hazem Mohammad Al-Kaseasbeh, & Almuhannad Alorf. (2023). The effect of quality, security and privacy factors on trust and intention to use egovernment services. *International Journal of Data and Network Science*, 185-198.

[12] Klinger, E, Wiesmaier, A, & Heinemann, A. (2022). A Review of Existing GDPR Solutions for Citizens and SMEs. *Hochschule Darmstadt - University of Applied Sciences, Germany*, 1-46.

[13] Liu, D., & Lemuria Carter. (2018). Impact of Citizens' Privacy Concerns on e-Government Adoption. *Association for Computing Machinery*, 1-6.

[14] Martínez-Navalón, J.-G., María FernándezFernández, & Fernanda Pedrosa Alberto. (2023). Does privacy and ease of use influence user trust in digital banking applications in Spain and Portugal? *International Entrepreneurship and Management Journal*, 781–803.

[15] Mutimukwe, C., Ella Kolkowska, & Åke Grönlund. (2017). Trusting and Adopting E-Government Services in Developing Countries? Privacy Concerns and Practices in Rwanda. *IFIP International Federation for Information Processing* , 324-335.

[16] Omoogun, M., Preetila Seeam, Visham Ramsurrun, Xavier Bellekens, & Amar Seeam. (2017). When eHealth Meets the Internet of Things: Pervasive Security and Privacy Challenges. *International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*, (pp. 1-7). London, UK.

[17] SADKI, S., & Hanan EL BAKKALI. (2014). Towards controlled-privacy in e-health: A comparative study. *International Conference on Multimedia Computing and Systems (ICMCS)* (pp. 674-679). Marrakech, Morocco: IEEE.

[18] Weinberger, M., Dan Bouhnik, & Maayan Zhitomirsky-Geffet. (2017). Factors Affecting Students' Privacy Paradox. *Open Information Science*, 3-20.

[19] Weinberger, M., Maayan Zhitomirsky-Geffet , & Dan Bouhnik. (2017). Sex differences in attitudes towards online privacy and anonymity among Israeli students with different technical backgrounds. *information research*, 1 -23.

[20] 2B Advice (2024) 2B Advice. Available at: https://www.2b-advice.com (Accessed: 18 August 2024, 10:00 AM).

[21] AvePoint Privacy Impact Assessment (PIA)

[22] AvePoint (2024) AvePoint Privacy Impact Assessment (PIA). Available at: https://www.avepoint.com (Accessed: 19 August 2024, 11:30 AM).

[23] BigID (2024) BigID. Available at: https://www.bigid.com (Accessed: 21 August 2024, 9:45 AM).

[24] IBM (2024) IBM OpenPages Data Privacy Management. Available at: https://www.ibm.com (Accessed: 23 August 2024, 8:15 AM).

[25] OneTrust (2024) OneTrust PreferenceChoice. Available at: https://www.onetrust.com (Accessed: 25 August 2024, 9:00 AM).

[26] Securiti.ai (2024) Securiti.ai. Available at: https://www.securiti.ai (Accessed: 27 August 2024, 10:30 AM).

[27] TrustArc (2024) TrustArc. Available at: https://www.trustarc.com (Accessed: 29 August 2024, 8:45 AM).

[28] Crownpeak (2024) Crownpeak. Available at: https://www.crownpeak.com (Accessed: 30 August 2024, 10:00 AM).

[29] DataPrivacyManager (2024) DataPrivacyManager. Available at: https://www.dataprivacymanager.net (Accessed: 1 September 2024, 9:30 AM).

[30] Ethical Data (2024) Ethical Data. Available at: https://www.ethicaldata.net (Accessed: 3 September 2024, 10:15 AM).

[31] Protiviti (2024) Protiviti. Available at: https://www.protiviti.com (Accessed: 5 September 2024, 11:45 AM).