International Journal of Information Science and Management
Vol. 24, No. 2, 2026, 105-124
DOI: / DOR:

Original Research

Digital Privacy Policies of Malaysian Public Libraries

Mohamad Noorman Masrek
Professor, Faculty of Information Science, Universiti Teknologi MARA Shah Alam Campus, Malaysia.
Corresponding Author:
mnoorman@uitm.edu.my
ORCID iD:
https://orcid.org/0000-0002-2730-5555

Qamarul Nazrin Harun
Ph. D. Candidate, Faculty of Information Science, Universiti Teknologi MARA Shah Alam Campus, Malaysia.
qamarulnazrin@uitm.edu.my
ORCID iD:
https://orcid.org/0000-0003-1645-0607

Received: 25 August 2024
Reviewed: 01 March 2025
Accepted: 17 February 2026

Abstract

This study examines the privacy practices of Malaysian public libraries by evaluating their compliance with the General Data Protection Regulation (GDPR). Using a qualitative content analysis approach, privacy statements from 15 major public libraries—including the National Library and 14 State Public Libraries—were assessed against 11 GDPR-based privacy criteria. The results reveal substantial variation in compliance. While all libraries (100%) disclosed data collection practices and policy changes, critical aspects such as privacy breach notification (0%), data aggregation (0%), protection of children's privacy (6.7%), and privacy settings (6.7%) were largely neglected. The highest-performing library met 81.8% of the criteria, while the lowest scored just 18.2%. These findings highlight a significant gap between current practices and international standards. The study recommends that Malaysian public libraries revise their privacy policies to address deficiencies in user control, data security, data retention, and breach response, thereby aligning more closely with global best practices and safeguarding patron privacy more effectively.

Keywords: Privacy Practice, Public Library, Malaysia, General Data Protection Regulation (GDPR), Digital Privacy Policies.

Introduction

Privacy has become a top concern for individuals and organizations in the era of digital information and communication. Libraries, as key providers of information resources and digital services, have a professional and ethical duty to safeguard user data and uphold privacy rights (Hess, LaPorte-Fiori & Engwall, 2015). This obligation is especially critical for public libraries, which serve diverse user groups and play an essential role in promoting equitable access to information. However, modern libraries face numerous challenges in ensuring that their websites and supporting technical infrastructure meet high standards of privacy and security (Breeding, 2019). Striking the right balance between offering improved, personalized services and protecting user privacy remains a complex task. Libraries are increasingly adopting digital tools to enhance user experiences and foster deeper engagement with patrons, but these

developments also raise concerns about how personal data is collected, managed, and protected (Wang, 2022). As Panda and Kaur (2023) note, this dual pursuit often creates tensions between innovation and privacy protection, requiring libraries to carefully navigate conflicting priorities.

Although global research has explored the adequacy and transparency of institutional privacy policies, little is known about how Malaysian public libraries articulate and implement their privacy practices. Prior studies have highlighted significant deficiencies in the availability, clarity, and compliance of privacy statements across government, municipal, and educational websites (Alhomod & Shafi, 2012; Dias, Gomes & Zúquete, 2016; Kautto & Henttonen, 2017). In library settings, similar shortcomings have been observed: privacy policies are often superficial, outdated, or noncompliant with professional guidelines (Kumar & Verma, 2018; Hussey, 2020; Valentine & Barron, 2022). These findings raise questions about the extent to which Malaysian public libraries align their practices with internationally recognized frameworks, particularly the General Data Protection Regulation (GDPR) (Intersoft Consulting, 2018). Given that Malaysian public libraries typically rely on the Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2015 as a guiding framework—predating the GDPR—there is a pressing need to evaluate how closely their website privacy statements reflect the more comprehensive and user-centric standards of the GDPR

Despite these important contributions, there is a notable lack of empirical research examining how Malaysian public libraries articulate and implement their online privacy policies. Specifically, little is known about the extent to which these policies align with internationally recognized standards, such as the General Data Protection Regulation (GDPR) (Intersoft Consulting, 2018). As a comprehensive EU framework, the GDPR offers a robust reference for evaluating privacy practices related to data collection, consent, retention, and user rights. However, the content and structure of privacy statements on Malaysian public library websites often appear vague or inconsistent, raising concerns about how well user data is protected and how clearly privacy responsibilities are communicated.

To address these gaps, there is a pressing need to examine and evaluate the privacy practices of Malaysian public libraries. Such research should assess the transparency and completeness of publicly available privacy statements, identify patterns and inconsistencies across institutions, and explore opportunities to improve user awareness and control over personal data. These efforts are essential not only to align with global best practices but also to strengthen user trust and institutional accountability in the digital era. In light of this, the study aims to assess the extent to which the privacy statements of Malaysian public libraries align with the General Data Protection Regulation (GDPR). To guide this investigation, the following research questions are posed:

- RQ1: To what extent do the privacy statements of selected Malaysian public libraries comply with the provisions of the GDPR?
- RQ2: What are the strengths and areas for improvement in the privacy practices of these libraries based on their published statements?

These questions are addressed through the following research objectives:

- RO1: To analyze and compare selected Malaysian public libraries' privacy statements with the provisions of the General Data Protection Regulation (GDPR).
- RO2: To identify areas of strength and potential improvement in selected Malaysian public libraries' privacy practices as reflected in their privacy statements.

Literature Review

Privacy policy

As digital engagement becomes increasingly pervasive, the role of privacy policies in safeguarding personal data has become more critical than ever. These policies serve not only as legal instruments but also as mechanisms for fostering user trust and ensuring transparency in how personal information is collected, used, and managed (Javed & Sajid, 2024; Valentine & Barron, 2022). Originating in the late 1990s and early 2000s with the rise of the internet, privacy policies have since become a standard component of most websites, reflecting growing concerns over digital data practices. Inadequate or absent privacy policies can expose organizations to legal repercussions, damage their reputations, and erode user trust (Shreiner, 2023; Chen, Shao & Zhu, 2025). More alarmingly, they may enable the mishandling or misuse of sensitive personal data, resulting in direct harm to individuals and liability for institutions (Hysa, D'Arco & Kostaqi, 2023). Hence, the presence of a clear, accessible, and well-articulated privacy policy is not merely a procedural requirement but a critical ethical and operational necessity for any data-collecting platform.

Despite their importance, many privacy policies fail to communicate effectively with end users. Mohan, Wasserman, and Chidambaram (2019) argue that these documents are often dense and overly technical, making them difficult for the average user to comprehend. This problem is compounded by excessive reliance on legal jargon and complex language, which discourages meaningful user engagement with the policy content (Javed & Sajid, 2024). As a result, users are frequently unaware of how their data is being handled, undermining the intent of transparency and informed consent. To address this gap, there is a clear need for more user-centric, accessible privacy policies that convey essential information in a straightforward, relatable manner.

Within the context of public libraries, this issue becomes especially relevant. Libraries are entrusted with upholding the confidentiality and privacy of their patrons—values that are fundamental to their mission. Yet, as libraries adopt digital services and web-based platforms, they encounter challenges in ensuring that these systems meet contemporary privacy and security standards (Shah & Hossain, 2022). There exists an inherent tension between the desire to deliver personalized, technology-driven services and the obligation to protect user privacy (Wang, 2022). Libraries must therefore navigate these competing demands carefully, balancing innovation with the ethical imperative of safeguarding user data.

General data protection regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive legal framework introduced by the European Union to safeguard individuals' privacy and personal data (Intersoft Consulting, 2018). It came into effect on May 25, 2018, and significantly transformed how organizations manage and protect user data, establishing a globally recognized standard for data governance. Its broad applicability, stringent requirements, and robust enforcement mechanisms have positioned the GDPR as a highly respected benchmark for evaluating privacy and security policies not only in Europe but worldwide. Due to its holistic approach, which includes core principles such as explicit consent, data minimization, and the right to erasure, it is frequently cited by scholars and researchers in privacy and data protection.

In the context of this study, the use of the GDPR as an evaluative benchmark is well justified, as it enables a structured and internationally grounded comparison of privacy

statements published by Malaysian public libraries. It also enhances the assessment's analytical rigor by aligning it with established standards for protecting user data and ensuring accountability in data practices. According to Mohan et al. (2019), the General Data Protection Regulation (GDPR) is grounded in a set of core data protection principles that govern the lawful and ethical processing of personal data. In line with Article 5 of the GDPR, these principles include lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. Together, these principles establish a comprehensive framework that not only regulates how personal data should be collected, processed, and retained, but also places explicit responsibility on data controllers to demonstrate compliance. Central to this framework is the concept of "data protection by design and by default," which emphasizes proactive compliance by integrating privacy-preserving safeguards into systems, processes, and organizational practices from the outset, rather than as a reactive measure. Informed by these principles, an ideal privacy policy, particularly for institutions such as public libraries, should clearly define the types of personal data collected, specify the intended purposes of collection, and explain the methods of data processing (Hintze, 2018). Prior to data collection, explicit consent from users should be obtained, empowering individuals to decide whether to share their information. The policy should also inform users of their rights under data protection law, including the right to access, rectify, or erase their personal data (Solove, 2022). In addition, it should outline the security measures adopted to protect user information and describe the procedures for responding to data breaches. By adopting a privacy policy that reflects these GDPR-aligned practices, organizations not only ensure legal compliance but also foster user trust and reinforce their commitment to ethical information management.

Malaysian public libraries websites

Almost all Malaysian public libraries refer to the circular Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2015 Pengurusan Laman Web Agensi Sektor Awam, issued by MAMPU in 2015, as a foundational guideline for developing privacy statements on their websites. This directive outlines detailed recommendations related to user privacy, personal information management, data collection, data aggregation, log data, cookie use, data protection protocols, website security, and policy updates. Notably, the provisions of the circular closely mirror several core elements of the General Data Protection Regulation (GDPR). Therefore, using GDPR as a benchmark for assessing the privacy statements of Malaysian public libraries is both relevant and appropriate.

By adhering to the principles outlined in the MAMPU circular, public libraries demonstrate an institutional commitment to addressing privacy concerns in alignment with recognized standards. The circular emphasizes critical aspects of privacy protection, including the handling of personal data, transparency in data usage, security safeguards, and notification of policy changes—all of which are central themes in the GDPR framework. However, while the circular provides a suitable structural foundation, full GDPR compliance demands more than policy articulation; it requires consistent implementation, regular review, and accountability. Therefore, a thorough evaluation is necessary to determine the extent to which these guidelines are actively practiced by libraries and whether appropriate measures are in place to protect patron privacy in real-world digital operations.

It is also important to acknowledge the disparity in web presence and digital capacity among public libraries in Malaysia. Although it is now standard practice for most libraries, regardless of size, to operate a website, the quality and maintenance of these sites vary significantly. The National Library and State Public Libraries typically manage well-designed, regularly updated websites with clear privacy notices and structured information architecture. In contrast, smaller public libraries, particularly those at the district or community level, often lack the necessary resources to maintain robust digital platforms. Their websites, if they exist at all, are usually basic in design, infrequently updated, and limited in the scope of information provided. This inconsistency in digital infrastructure poses a challenge to the comprehensive evaluation of privacy practices, as many smaller libraries may lack publicly accessible, well-documented privacy policies, even though they serve as important access points for local communities.

Past related studies on privacy statement assessment

Numerous studies have investigated the availability, content quality, and legal compliance of institutional privacy policies, offering valuable insights for evaluating privacy practices in public libraries, as shown in Table 1. Alhomod and Shafi (2012), for example, examined e-government websites in Saudi Arabia and found that only a small portion (28%) had privacy statements, and many failed to incorporate key elements of Fair Information Practice Principles. Similarly, Dias et al. (2016) found low adoption of privacy policies among Portuguese municipalities and highlighted major deficiencies in cookie disclosures and information on user rights. These patterns are echoed in Kautto and Henttonen's (2017) findings on Finnish municipal websites, where privacy statements were not only rare but also difficult to locate, suggesting that legal traditions alone are insufficient to ensure public access to privacy information.

In the Indian context, Kumar and Verma (2018) conducted a detailed content analysis of library websites from NAAC-accredited 'A' grade universities in the Central Zone of India. Their evaluation revealed that while most websites provided basic institutional and service information, they largely lacked essential elements, including privacy statements, feedback mechanisms, and OPAC integration. Advanced digital features like remote access, online catalogs, and institutional repositories were also generally absent. Among the institutions studied, Vikram University's library website ranked the highest, underscoring significant variation in digital transparency and service quality even within a small geographic cluster of institutions.

Internationally, research has also focused on compliance with established privacy frameworks, particularly the General Data Protection Regulation (GDPR). Vanezi, Zampa, Mettouris, Yeratziotis and Papadopoulos (2021) assessed the degree of GDPR alignment across web platforms and found substantial sectoral differences, with banking websites showing stronger compliance than educational ones. Fang and Yao (2018) revealed that even large multinational companies struggled to obtain valid user consent in accordance with GDPR requirements, often relying on implied or soft opt-in mechanisms. Lin, Liu, Li, Xiong and Gou (2022) offered a dual-layered evaluation of Chinese websites by comparing stated policies with actual behaviors and found significant discrepancies—especially concerning third-party tracking and cookie retention—indicating a superficial approach to compliance.

In the context of libraries and academic institutions, the situation appears similarly inconsistent. Lund (2021) reported that over half of U.S. public libraries lacked publicly accessible data privacy policies, despite increasing public concern over data protection. Valentine and Barron (2022) evaluated privacy policies of U.S. academic libraries and found very low adherence to the American Library Association's privacy guidelines. Only a few institutions included comprehensive details such as breach notifications or server infrastructure. Hussey (2020) noted the absence of a formalized privacy policy at Dominican University Library and recommended developing policies that reflect both national regulations and international frameworks such as the GDPR. These findings were supported by Bareh (2021), who found that although Indian academic websites demonstrated some technical protections such as HTTPS and TLS, they frequently lacked cookie disclosures and proper consent mechanisms.

Other studies have highlighted concerns related to policy clarity and accessibility. Javed, Al Qahtani, and Shehab (2021) found that privacy statements from banking and mobile money services in the Middle East were difficult to understand, with a readability level suitable only for those with higher education. Mukherjee and Gutierrez (2024) similarly found that New Zealand websites often failed to explain cross-border data disclosure and used vague language to describe safeguards, even when such policies were technically in place. These recurring issues-policy absence, lack of transparency, limited GDPR alignment, and poor readability-underscore the need for systematic evaluation of privacy practices in public-facing institutions.

Taken together, these prior studies offer an essential benchmark for analyzing Malaysian public libraries' privacy statements. They demonstrate the importance of not only assessing the presence and completeness of privacy disclosures but also examining their alignment with international standards such as the GDPR. In addition, identifying areas of strength and improvement-whether in policy accessibility, content detail, or compliance mechanisms-can inform efforts to enhance data protection practices and build public trust in library services.

Table 1
Past related studies

Author(s)	Objective	Method	Key Findings	Difference from the Present Study
Alhomod & Shafi (2012)	To examine the presence and quality of privacy policies in Saudi e-government websites	Content analysis of 54 sites using FIPs principles (Notice, Choice, Access, Security)	Only 28% had privacy statements; of these, 40% lacked sufficient coverage, indicating a low institutional emphasis on user privacy	Focused on e-government; no analysis of library websites or GDPR framework
Dias et al. (2016)	To assess the visibility and quality of privacy policies on Portuguese municipal websites	Observational survey and conceptual analysis of 308 sites	Only 26% had privacy policies; most lacked cookie notices, and many transmitted login data insecurely	Centered on municipal sites in Portugal; no comparison with international frameworks like GDPR
Kautto & Henttonen (2017)	To evaluate whether Finnish municipal websites displayed	Web content scan (309 sites) and internal search queries (38 sites)	Privacy links were rare or buried; statements were outdated or difficult to locate,	Investigated FOI policies broadly, not library or GDPR-specific evaluation

Author(s)	Objective	Method	Key Findings	Difference from the Present Study
	FOI and privacy policies		despite strong national data laws	
Fang & Yao (2018)	To analyze corporate GDPR compliance via website consent mechanisms	Content analysis of 125 major international websites	Fewer than 30% collected valid consent; implied and soft opt-in methods are still common, despite GDPR	Focused on corporate and commercial websites; did not assess public institutions
Harrell (2018)	To compare privacy coverage in public vs private sector websites	Qualitative policy content analysis	Government sites were more user-centered and accessible; private sector policies were vague and compliance-oriented	Not library-specific; no cross-national benchmarking, such as GDPR, used
Kumar & Verma (2018)	To evaluate the content of library websites from NAAC-accredited 'A' grade universities in Central India	Content analysis using a checklist: quantifying the score of site quality	Vellore University scored the highest for content quality. Most sites lacked privacy statements, OPACs, feedback forms, and digital services	Focused on academic libraries; did not benchmark privacy against GDPR
Reddick & Zheng (2018)	To assess online privacy protection on Chinese city websites	Benchmarking index applied to 100 city websites	Only 37% published privacy statements; compliance levels correlated with city GDP and size	Focused on Chinese city-level websites; no focus on library services or user trust dimensions
Avuglah, Owusu-Ansah, Tachie-Donkor & Yeboah (2020)	To examine privacy practices in academic libraries in Ghana from both librarian and student perspectives	Survey of 74 librarians and 726 students using structured questionnaires and content analysis of open-ended responses	Low awareness of privacy policies, limited training and communication, and few public initiatives; calls for education, stronger policies, and awareness	Focused on academic libraries and user perceptions, the present study assesses Malaysian public libraries' website statements against GDPR
De & Shukla (2020)	To evaluate how Indian e-governance app policies reflect legal privacy standards	Policy review and user interviews	Policies lacked core elements; users had trust but poor awareness of privacy implications	Focused on mobile governance apps, not libraries or GDPR benchmarking
Hussey (2020)	To examine the presence of library-specific privacy policies in U.S. academic institutions	Case study with comparative content analysis of 12 library websites	Most libraries had no dedicated privacy policy; key areas like social media and GDPR were often omitted	U.S.-based academic libraries did not use EU GDPR as an evaluative framework
Vaughan (2020)	Examines libraries' role in protecting user privacy post-GDPR	Conceptual analysis based on professional ethics and privacy norms	Highlights the need for stronger institutional privacy practices and user awareness	Focuses on ethical discourse, while the present study offers an empirical analysis of Malaysian library websites
Vos, Hu & Du (2020)	To explore privacy notices on NZ organizations' Facebook pages	Content analysis of 200 organizational pages	Only 16% had any privacy notice; user data collected via social	Focused on social media platforms, not formal website policies or libraries

Author(s)	Objective	Method	Key Findings	Difference from the Present Study
			features was rarely disclosed	
Bareh (2021)	To evaluate privacy and security practices on Indian academic websites	Webometric review of 130 sites	TLS and HTTPS were implemented, but cookie consent was absent; policies lacked readability and clear user protections	Emphasized cybersecurity layers, not legal compliance, such as GDPR
Ambika & Ganesan (2021)	To rank Indian central university library websites based on content quality	29-point web content checklist on 13 libraries	Only one library rated excellent; many lacked clear mission statements, copyright info, or privacy-related content	Ranked based on generic web quality, not privacy content depth or GDPR conformity
Lund (2021)	To assess the presence and quality of U.S. public library privacy statements	Content and cluster analysis of 1,000 websites	More than half of libraries had no published privacy policy; need for clear, visible, and regularly updated policies	Focused on volume and presence of policies in the U.S.; no benchmarking against GDPR
Javed et al. (2021)	To measure privacy compliance and readability of finance-related privacy policies	Manual review of 55 policies using GSMA/FDIC benchmarks	Banks had stronger compliance than mobile services; overall readability was poor, and excluded youth/lay users	Examined the finance sector with non-GDPR benchmarks; not focused on libraries
Vanezi et al. (2021)	To evaluate GDPR alignment in privacy statements across sectors	Automated tool analyzing 148 websites using GDPR-based keyword taxonomy	Compliance varied; the banking sector performed best, the education sector performed weakest; some key rights, like rectification, were often missing	Broad cross-sector comparison; education sector insights not library-specific
Lin et al. (2022)	To examine consistency between privacy statements and real web behavior	Combined automated policy review and passive behavior tracking across 663 Chinese websites	Only a fraction honored their own privacy claims; internal tracking often contradicted published policies	Tested behavioral integrity, not just document analysis; context is Chinese commercial sites
Valentine & Barron (2022)	To examine academic library privacy statements for ALA compliance and new issues	Deductive coding using ALA standards plus emergent theme analysis (78 libraries)	No library fully complied; new themes like analytics and institutional data sharing emerged, but lacked transparency	Based on ALA, not GDPR; focused on thematic emergence in academic libraries only
Farid, Warraich, & Iftikhar (2023)	To examine how library privacy policies align with GDPR principles	Systematic Literature Review (SLR) of GDPR applications in library contexts	Identified a lack of GDPR compliance in library privacy policies globally; stressed the need for awareness and policy reform	SLR-based; the present study is empirical, focusing on actual privacy statements of Malaysian public libraries

Author(s)	Objective	Method	Key Findings	Difference from the Present Study
Mukherjee & Gutierrez (2024)	To assess the compliance of New Zealand websites with the Privacy Act 2020	Structured checklist applied to privacy policies across six sectors	Strong alignment with core collection principles, but weak in areas like overseas data disclosure and policy specificity	Used New Zealand's Privacy Act, not GDPR; cross-sectoral rather than library-focused
Narimene & Mehdi (2024)	To explore data collection and sharing practices of Algerian e-commerce sites	Quantitative content analysis of 126 websites	Personal data was widely collected; data sharing with partners was common, but disclosures remained vague and lacked user control options	Focused on e-commerce, not public services; policy analysis limited to user control, not GDPR compliance

Materials and Methods

The study focused on Malaysian public libraries. Out of the approximately 13,062 libraries in the country (IFLA, 2019)-including school libraries, academic libraries, special libraries, community libraries, and public libraries-a purposive sampling technique was employed to select fifteen (15) libraries (Table 2), comprising the National Library of Malaysia and the 14 State Public Libraries. These institutions were intentionally chosen because they represent the highest-level public library authorities in each state and collectively provide a comprehensive national perspective on public library privacy practices. Purposive sampling is appropriate in qualitative content analysis when the objective is to examine a specific category of institutions or information environments in depth (Kumar & Verma, 2018; Javed, Salehin, & Shehab, 2020). By focusing on state-level public libraries, the study ensures that the sample reflects the most prominent and administratively significant entities within the Malaysian public library system.

Table 2
List of libraries assessed

No.	Library Name	Governance Level	Website URL
1	National Library of Malaysia	National	https://www.pnm.gov.my
2	Perbadanan Perpustakaan Awam Selangor (PPAS)	State	https://www.ppas.gov.my
3	Perbadanan Perpustakaan Awam Kedah (PPAK)	State	https://www.kedahlib.gov.my
4	Perbadanan Perpustakaan Awam Pulau Pinang (PPAPP)	State	https://www.penanglib.gov.my
5	Perbadanan Perpustakaan Awam Negeri Sembilan	State	https://www.ns.library.gov.my
6	Perbadanan Perpustakaan Awam Terengganu	State	https://www.trglib.gov.my
7	Perbadanan Perpustakaan Awam Kelantan	State	https://www.kelantanlib.gov.my
8	Perbadanan Perpustakaan Awam Melaka	State	https://www.perpustam.gov.my
9	Perbadanan Perpustakaan Awam Johor	State	https://www.ppaj.gov.my

No.	Library Name	Governance Level	Website URL
10	Perbadanan Perpustakaan Awam Perak	State	https://www.peraklibrary.gov.my
11	Perbadanan Perpustakaan Awam Pahang	State	https://www.pahanglibrary.gov.my
12	Perbadanan Perpustakaan Awam Sabah	State	https://www.sabah.library.gov.my
13	Perbadanan Perpustakaan Awam Sarawak	State	https://www.pustaka-sarawak.com
14	Perbadanan Perpustakaan Awam Wilayah Persekutuan	Federal Territory	https://www.dbkl.gov.my/ms/pustaka
15	Perbadanan Perpustakaan Awam Perlis	State	https://www.perlislib.gov.my

This study adopted a content analysis strategy, a well-established and widely used qualitative research method for systematically interpreting textual data. Content analysis enables researchers to transform unstructured data into meaningful, organized insights by identifying patterns and themes (Krippendorff, 2018). It is especially effective for analyzing website content, policy documents, and textual representations of organizational practices. Importantly, the assessment was conducted entirely by the researchers themselves, without involving any external experts. This approach is common and accepted in similar studies on web-based policy evaluations, where researchers apply predefined coding schemes to ensure consistency and objectivity (Javed et al., 2020; Kumar & Verma, 2018). Researcher-led evaluations allow direct control over coding reliability and are particularly useful when the coding framework is well established.

The thematic framework for content analysis in this study was not developed from scratch. Instead, it was adapted from Tesfay, Hofmann, Nakamura, Kiyomoto and Serna (2018), whose work provides a comprehensive and structured thematic model for evaluating internet privacy policies. While the GDPR defines seven high-level data protection principles under Article 5, these principles are normative and abstract. As such, direct empirical assessment requires translating them into observable, operational privacy criteria. Accordingly, the themes adopted in this study represent GDPR-based operational aspects rather than the formal GDPR principles themselves. These aspects are grounded in GDPR requirements and guidance, thereby ensuring a strong conceptual linkage to the regulation while remaining suitable for systematic document analysis.

Each privacy statement from the fifteen selected Malaysian public libraries was systematically analyzed using predefined GDPR-based themes. Specifically, the analysis employed 11 GDPR-based privacy aspects—data collection, protection of children, third-party sharing, data security, data retention, data aggregation, control of data, privacy settings, account deletion, privacy breach notification, and policy changes—which reflect how GDPR principles such as transparency, lawfulness, integrity and confidentiality, purpose limitation, and accountability are operationalised and communicated in practice through publicly available privacy statements. The assessment examined how comprehensively each theme was addressed in the statements, enabling detailed comparisons across libraries.

To ensure reliability, the researchers independently coded the data and cross-compared their findings, resolving any discrepancies through discussion. This process enhanced

consistency and minimized potential bias. As the study did not involve human participants or sensitive data, ethical approval was not required. The analysis was confined to publicly accessible documents, and all stages of the research were conducted in adherence to principles of academic integrity and respect for intellectual property.

Results

Table 3 offers a detailed overview of the privacy assessment conducted on all fifteen Malaysian public libraries, with reference to the GDPR The assessment includes several components, beginning with data gathering. It should be noted that each public library has taken the step of publicly clarifying its data-gathering procedures on its own website, ensuring transparency in its operations. Moving on to the next aspect, the protection of children's privacy, only one public library has explicitly stated the criterion for this on its website. The remaining 14 libraries, on the other hand, have made no clear mention of, or provided information directly addressing, this critical topic. This underscores the need for greater attention and effort to protect minors' privacy in all public libraries.

Regarding the third aspect, data sharing, the majority of libraries (11 out of 15) have taken the proactive step of explicitly stating their data-sharing policy on their websites. This commitment to transparency and openness in information sharing demonstrates their commitment to protecting the privacy and security of their customers' data. When it comes to data security, the evaluation found a fairly equal split between libraries that provide explicit information on this topic and those that do not. Eight of the fifteen public libraries assessed have taken the laudable step of addressing data security risks. These libraries have stated unequivocally that any data acquired from their patrons will be treated with the highest confidentiality, ensuring that the information is strictly secured and not shared or distributed to any third parties. The proactive approach to data security displayed by these eight libraries instills trust and confidence in its patrons. Visitors to the library can be certain that their personal information will be treated with the utmost care, adding to their peace of mind. It is worth mentioning, however, that the remaining seven libraries have not offered detailed rules on data protection. This suggests a possible area for improvement, as open communication about data security measures is critical for creating a secure and trustworthy environment for library patrons.

Data retention is an important aspect addressed by the GDPR, although many public libraries in Malaysia may not fully appreciate its relevance, as the bulk of libraries' websites do not promote this feature. Only a few libraries (five out of 15) have openly stated their data retention policies, while the remaining libraries have not provided any information in this regard. In addition to data retention, another important aspect to consider is data aggregation. Data aggregation, as defined by the GDPR, is the collecting, compilation, and analysis of data from numerous sources to provide aggregated or summary information. Surprisingly, none of the assessed libraries' websites expressly state this criterion. Incorporating information regarding data aggregation processes can help to promote openness and provide library patrons a better understanding of how their personal data is collected and used.

Data control is an important feature that demands attention and transparency, but it is conspicuously absent from the bulk of public library websites. Only three of the 15 libraries evaluated have taken the initiative to provide explicit information about data control on their websites. This restricted representation emphasizes the importance of data control policies in

the public library landscape. The absence of proper emphasis on privacy settings is also troubling. According to the data, only one library has provided extensive information on privacy settings, while the rest have not adequately addressed this essential topic. Privacy settings play an important role in allowing individuals to control how their personal information is displayed and accessible, ensuring their privacy preferences are respected.

Account deletion and reporting of privacy breaches are two critical issues underlined by the GDPR, yet their importance appears to be disregarded by most public libraries. Only two of the 15 libraries evaluated have taken the initiative to handle account deletion on their websites, suggesting a likely lack of awareness among the remaining libraries of the necessity of this function. Equally troubling is the absence of focus on privacy breach notification across all public libraries reviewed. The lack of privacy breach notification material on their websites indicates a wasted opportunity to inform users about how the libraries handle and respond to potential breaches of their personal data.

Policy changes, the final feature reviewed in this study, have been widely acknowledged by all libraries, as indicated by their explicit inclusion on each library's website. It is admirable that every library has realized the necessity of notifying its patrons about policy changes, exhibiting a commitment to transparency, and keeping its users informed.

Table 3
Results of assessment

	Public Library														
Aspect of Assessment	PL1	PL2	PL3	PL4	PL5	PL6	PL7	PL8	PL9	PL10	PL11	PL12	PL13	PL14	PL15
Data collection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protection of Children	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No
Third-Party Sharing	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Data Security	No	Yes	Yes	No	Yes	No	No	Yes	No	Yes	No	Yes	Yes	Yes	No
Data Retention	No	No	No	No	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No
Data Aggregation	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Control of Data	No	No	No	No	Yes	No	No	No	No	Yes	No	Yes	No	No	No
Privacy Setting	No	No	No	No	Yes	No	No	No	No	No	No	No	No	No	No
Account Deletion	No	No	No	No	Yes	No	No	No	No	Yes	No	No	No	No	No
Privacy Breach Notification	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Policy Changes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Legend: "Yes" indicates that the specific GDPR-aligned privacy aspect is explicitly addressed in the library's privacy statement. "No" indicates that the aspect is absent or not explicitly stated in the privacy statement.															

Table 4 presents the extent of compliance with GDPR privacy elements across the 15 public libraries assessed. The highest compliance was recorded by PL5, which addressed 9 out of the 11 privacy aspects (81.8%), indicating strong alignment with international privacy standards. In contrast, PL4, PL9, and PL15 demonstrated the lowest compliance, addressing only two

aspects (18.2%). Most libraries, including PL1, PL2, PL6, PL7, and PL11, complied with approximately 3 aspects (27.3%). These results indicate a substantial disparity in privacy policy practices among Malaysian public libraries.

Table 4
GDPR compliance percentage by individual library

Library	Total "Yes" Aspects	Percentage of Compliance (%)
PL1	3	27.3%
PL2	3	27.3%
PL3	4	36.4%
PL4	2	18.2%
PL5	9	81.8%
PL6	3	27.3%
PL7	3	27.3%
PL8	4	36.4%
PL9	2	18.2%
PL10	6	54.5%
PL11	3	27.3%
PL12	5	45.5%
PL13	4	36.4%
PL14	4	36.4%
PL15	2	18.2%
Note: The libraries listed in Table 2 are presented with their actual names. However, in the findings section, pseudonyms (e.g., PL1, PL2) are used in a different order to maintain confidentiality and avoid any direct association between the actual libraries and their evaluated privacy practices.		

Table 5 summarizes the compliance level for each GDPR privacy aspect. All 15 libraries (100%) disclosed data collection practices and policy changes, indicating high transparency in these areas. However, several critical privacy dimensions were largely absent, such as data aggregation and privacy breach notification, which received 0% compliance. Similarly, aspects such as the protection of children's privacy (6.7%), account deletion (13.3%), and privacy settings (6.7%) were poorly addressed. On average, each privacy aspect was complied with by only 5.5 libraries (36.7%), suggesting that most libraries meet fewer than half of the key privacy requirements outlined in the GDPR.

Table 5
GDPR compliance by privacy aspect

Privacy Aspect	Total (Yes)	Percentage (%)
Data Collection	15	100.0%
Protection of Children	1	6.7%
Third-Party Sharing	11	73.3%
Data Security	8	53.3%
Data Retention	5	33.3%
Data Aggregation	0	0.0%
Control of Data	3	20.0%

Privacy Aspect	Total (Yes)	Percentage (%)
Privacy Setting	1	6.7%
Account Deletion	2	13.3%
Privacy Breach Notification	0	0.0%
Policy Changes	15	100.0%
Mean	5.5	36.7%

Discussion

RO1: Comparative analysis of library privacy statements with GDPR provisions

The findings of this study demonstrate that while Malaysian public libraries have made some progress in enhancing privacy transparency, overall compliance with the General Data Protection Regulation (GDPR) remains inconsistent and limited. Full compliance was observed only for two aspects-data collection and policy change notifications-with all 15 libraries addressing these. However, substantial gaps persist across other core GDPR requirements.

The universal disclosure of data collection practices is consistent with international trends, where such practices often receive the most visibility in privacy statements (Fang & Yao, 2018; Reddick & Zheng, 2018). Similarly, consistent inclusion of policy change notifications reflects procedural transparency, a common feature in many government websites (Harrell, 2018). These findings align with Vaughan's (2020) argument that libraries are ethically bound to uphold privacy protections but often meet only the most basic requirements, frequently falling short in areas that demand deeper user engagement or technical specificity.

Low compliance in critical areas such as children's privacy protection (6.7%), account deletion (13.3%), privacy settings (6.7%), and breach notifications (0%) highlights a lack of comprehensive user-centered controls. This mirrors findings from Valentine and Barron (2022), who observed that U.S. academic libraries often failed to meet ALA privacy guidelines, particularly regarding data security and third-party access. Similar issues were identified in Farid, Warraich, and Iftikhar's (2023) systematic review, which found that library privacy policies-especially in the Global South-rarely reflect GDPR's holistic principles, emphasizing instead general statements over actionable details.

The complete absence of breach notification mechanisms is especially concerning. This reinforces global observations such as those by De and Shukla (2020), who highlighted institutional weaknesses in Indian e-government apps due to non-disclosure of security incidents. Kautto and Henttonen (2017) also noted that breach-related information was often inaccessible or outdated on Finnish municipal websites. Vaughan (2020) further critiques this lack of proactive communication, suggesting that many libraries struggle to balance operational transparency with evolving privacy obligations.

Equally troubling is the absence of data-aggregation disclosures across all 15 libraries. As Lund (2021) pointed out in his study of U.S. public library websites, privacy policies rarely mention profiling, analytics, or cross-platform data use-despite their growing relevance in library systems. This gap signals not only an oversight in addressing modern privacy risks but also a disconnect between policy language and actual digital practices.

With an average compliance rate of 36.7% per privacy aspect (as shown in Table 5), Malaysian public libraries appear to lag behind more regulated sectors, such as banking. Vanezi et al. (2021) reported stronger GDPR alignment in financial institutions, particularly regarding core user rights such as data access and rectification—features often absent from education-

related policies. This sectoral underperformance is also echoed by Farid, Warraich, and Iftikhar (2023), who emphasized the need for tailored training and policy reform in the library sector to elevate compliance levels.

RO2: Strengths and areas for improvement in privacy practices

The assessment of the privacy statements of Malaysian public libraries reveals a mixed pattern of strengths and critical areas requiring improvement. Drawing on the comparative results across the 11 GDPR-aligned privacy aspects (as shown in Tables 4 and 5), the findings show encouraging progress in foundational transparency; however, significant deficiencies persist in areas that demand proactive user protection and responsive risk communication.

A key strength lies in the universal disclosure of data collection practices. All 15 libraries clearly outlined the types of personal data being collected, aligning well with the GDPR's transparency principles. This echoes patterns reported by Alhomod and Shafi (2012) and Dias et al. (2016), in which data collection remained one of the most frequently documented privacy practices, even in contexts with otherwise limited policy depth. Likewise, the consistent presence of policy change notifications across all libraries indicates a growing institutional awareness of the importance of procedural updates—a point also noted by Harrell (2018) in her assessment of privacy responsiveness across public-sector websites.

Nevertheless, the analysis also identifies several critical weaknesses. Chief among them is the complete absence of privacy breach notification mechanisms, a fundamental requirement under Article 33 of the GDPR. The lack of any mention of such procedures suggests institutional unpreparedness for a data compromise. Ong (2023) underscores that breach notification is both a legal and ethical imperative—serving not only as a transparency tool but also as a signal of organizational accountability. The omission of this feature across all libraries significantly undermines public trust.

Equally troubling is the minimal attention paid to children's privacy. Only one library (6.7%) explicitly addressed this sensitive issue, despite the high proportion of young users in the public library system. Valentine and Barron (2022) observed a similar neglect among ARL libraries in the U.S., where protections for children were scarcely included despite institutional mandates. Vaughan (2020) also raises concern that libraries, while historically seen as privacy advocates, often fail to implement robust child-specific data safeguards—particularly in the digital realm. This reinforces the urgency for Malaysian public libraries to revisit their ethical obligations in light of regulatory requirements.

In terms of user autonomy, only three libraries (20%) provided mechanisms for data control-such as accessing, modifying, or deleting personal data. This low representation of user rights mirrors findings from Narimene and Mehdi (2024), who noted that platforms in Algeria often emphasized data collection but offered limited user control. In library contexts, Vaughan (2020) argues that the lack of visible user empowerment mechanisms erodes the perception of libraries as safe, neutral digital spaces. Without clear avenues for data correction or deletion, patrons may become reluctant to fully engage with digital services.

The study further identified limited attention to account deletion, privacy settings, and data retention-areas where compliance ranged from 6.7% to 33.3%. These dimensions are central to informed consent and responsible data stewardship. Lund (2021) similarly found that even technologically advanced U.S. public libraries often lacked detail in these areas, suggesting that institutional inertia and technical complexity may be universal barriers.

Finally, the total absence of disclosures on data aggregation—how user data might be combined or analyzed for internal or third-party purposes—is a growing concern. This finding mirrors Vos, Hu, and Du's (2020) work, which highlighted that organizations rarely articulate their profiling or analytics practices, even as these tools become more prevalent. Given that libraries increasingly rely on analytics for improving services, failing to disclose these practices compromises the principles of openness and user awareness. Vaughan (2020) emphasizes that modern privacy policies must go beyond passive disclosures and actively educate users about how their data is used across systems—a dimension largely absent in the libraries reviewed.

Interestingly, even among libraries that demonstrated stronger overall compliance (e.g., PL5 with 81.8%), the missing components tended to involve user-centric and incident-driven privacy protections. This suggests a broader pattern in which foundational transparency is increasingly normalized, yet deeper commitments to user empowerment and accountability remain insufficiently developed.

Conclusions

The assessment of Malaysian public library privacy statements through the lens of the General Data Protection Regulation (GDPR) reveals a layered and uneven adoption of privacy-related best practices. While a consistent commitment to basic transparency—such as disclosing data collection and notifying policy changes—was observed across all libraries, deeper user-centric protections remain largely unaddressed. This partial compliance reflects a surface-level engagement with privacy protocols rather than a comprehensive implementation of international standards.

In relation to RQ1 and RO1, the findings indicate that although libraries recognize the need to publish privacy statements, their content often lacks the granularity and precision expected under GDPR. Critical components such as breach notifications, privacy settings, and children's data protection are either completely absent or minimally represented. This suggests that the statements serve more as formalities than as actionable commitments to privacy governance.

With respect to RQ2 and RO2, the study uncovered significant discrepancies in how different libraries address the same privacy aspects. Even among institutions with higher levels of digital infrastructure, such as state libraries, the implementation of privacy measures remains inconsistent. This variation signals a lack of standardized policy development and suggests that compliance is driven more by institutional discretion than by coordinated governance frameworks. Importantly, the absence of key GDPR elements—even in libraries with otherwise strong digital presence—points to an institutional underestimation of the operational implications of privacy assurance.

Contribution

This study contributes to the ongoing discourse on privacy governance by offering actionable strategies to strengthen data protection practices across Malaysian public libraries. Based on the identified gaps, it is recommended that libraries revise and standardize their privacy policies, particularly those published on their websites, to align with international frameworks such as the GDPR. Key areas requiring immediate attention include protecting children's data, implementing breach notification protocols, establishing clear data retention and deletion policies, enhancing user control mechanisms, and ensuring transparency in data aggregation and sharing practices. To support implementation, centralized bodies such as the National Library should develop standard website policy templates and toolkits that can be adapted by state and district-level libraries, especially those with limited technical or financial

resources. Public libraries should also prominently display their privacy notices on their websites, ensure the content is accessible and comprehensible to all users, and include interactive elements, such as consent options and simplified user settings.

In parallel, it is crucial to build institutional capacity through regular staff training on privacy laws, ethical data handling, and secure digital practices, particularly those related to managing user interactions on websites. This recommendation is directly informed by the findings of our study, which revealed significant gaps in key GDPR-aligned areas such as breach notification, children's privacy protection, and user data control. Addressing these deficiencies requires not only policy updates but also equipping library personnel with the knowledge and skills necessary to implement and sustain these privacy measures effectively.

Designating dedicated personnel-such as Data Protection Officers-within each library or library network can facilitate compliance monitoring and improve incident response (Šidlauskas, 2021). Regular internal audits or privacy assessments should also be conducted to evaluate website content and compliance with privacy standards, thereby guiding ongoing policy enhancements. In addition, fostering collaboration among libraries through national forums can enable shared learning, harmonization of website policies, and the diffusion of best practices. These coordinated efforts will not only ensure that libraries meet evolving data protection standards but also reinforce their role as trusted public institutions that safeguard users' digital rights in an increasingly data-driven environment.

Limitations

This study was limited to an analysis of the National Library of Malaysia and 14 State Public Libraries. While this coverage provides insights into leading public institutions at the federal and state levels, it does not account for the broader ecosystem of community, academic, school, and special libraries across the country. Future research should include a larger and more diverse sample of libraries to develop a more comprehensive understanding of national privacy practices. Moreover, the analysis was based solely on publicly available privacy statements on library websites. It is possible that additional privacy safeguards exist but are not reflected in online documentation. Subsequent studies could incorporate interviews, surveys, or policy audits involving library administrators, IT staff, and patrons to triangulate findings and gain a deeper understanding of actual practices versus stated policies. Lastly, the study did not capture user perspectives on privacy. Future investigations should include patron feedback to assess their awareness, expectations, and trust in how their personal data is managed by libraries. This user-centered approach would provide valuable insights into the real-world impact of institutional privacy policies.

Reference

Alhomod, S. M. & Shafi, M. M. (2012). Privacy policy in e-government websites: A case study of Saudi Arabia. *Computer and Information Science,* 5(2), 88–94. https://doi.org/10.5539/cis.v5n2p88

Ambika, C. A. & Ganesan, P. (2021). Central university library websites in India: Web content analysis. *Library Philosophy and Practice (e-journal).* 5405. Retrieved from *https://digitalcommons.unl.edu/libphilprac/5405*

Avuglah, B. K., Owusu-Ansah, C. M., Tachie-Donkor, G. & Yeboah, E. B. (2021). Privacy practices in academic libraries in Ghana: Insight into three top universities. *IFLA Journal,* 47(2), 196–208. https://doi.org/10.1177/0340035220981061

Bareh, C. K. (2021). Assessment of the privacy and security practices of the Indian academic websites. *Library Philosophy and Practice,* 6426. Retrieved from https://digitalcommons.unl.edu/libphilprac/6426/

Breeding, M. (2019). Protecting privacy on library websites: Critical technologies and implementation trends. *Library Technology*, 55(7), 1-37. https://doi.org/10.5860/ltr.55n7

Chen, S., Shao, B. & Zhu, Y. (2025). The effectiveness of functional and affective recovery strategies in restoring user trust after privacy violations: The moderating role of violation type. *Information Technology & People*, 39(3), 1317-1340. https://doi.org/10.1108/itp-11-2024-1397

De, S. J. & Shukla, R. (2020). Privacy policies of e-governance initiatives: Evidence from India. *Journal of Public Affairs,* 20(4), e2160. https://doi.org/10.1002/pa.2160

Dias, G. P., Gomes, H. & Zúquete, A. (2016). Privacy policies and practices in Portuguese local e-government. *Electronic Government, an International Journal,* 12(4), 301–318. https://doi.org/10.1504/EG.2016.080430

Fang, S. & Yao, M. (2018). Investigating GDPR compliance across consumer-related websites: Are businesses telling consumers the truth about data collection? (working paper). Retrieved from https://hdl.handle.net/2142/103224

Farid, G., Warraich, N. F. & Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 51(4), 1000-1014. https://doi.org/10.1177/01655515231160026

Harrell, K. H. (2018). *A content analysis of governmental and private enterprise website privacy policies*. Master's paper. University of North Carolina at Chapel Hill, School of Information and Library Science. https://doi.org/10.17615/3sdz-r802

Hess, A. N., LaPorte-Fiori, R. & Engwall, K. (2015). Preserving patron privacy in the 21st-century academic library. *The Journal of Academic Librarianship,* 41(1), 105-114. https://doi.org/10.1016/j.acalib.2014.10.010

Hintze, M. (2018). Privacy statements under the GDPR. *Seattle University Law Review,* 42, 1129–1152. Retrieved from https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2603&context=sulr

Hussey, P. (2020). Why is an internet & information privacy policy necessary? *World Libraries,* 24(1). Retrieved from https://worldlibraries.dom.edu/index.php/worldlib/article/view/586/671

Hysa, X., D'Arco, M. & Kostaqi, J. (2023). Misuse of personal data: Exploring the privacy paradox in the age of big data analytics. In Anna Visvizi, Orlando Troisi, Mara Grimaldi (eds) *Big data and decision-making: Applications and uses in the public and private sector* (pp. 43–57). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80382-551-920231004

International Federation of Library Associations and Institutions (IFLA). (2019). *Library map of the world: Malaysia.* https://librarymap.ifla.org/countries/Malaysia

Intersoft Consulting. (2018). General Data Protection Regulation (GDPR). GDPR-Info.eu. https://gdpr-info.eu/

Javed, Y. & Sajid, A. (2024). A systematic review of privacy policy literature. *ACM Computing Surveys,* 57(2), 1-43. https://doi.org/10.1145/3698393

Javed, Y., Al Qahtani, E. & Shehab, M. (2021). Privacy policy analysis of banks and mobile money services in the Middle East. *Future Internet,* 13(1), 10. https://doi.org/10.3390/fi13010010

Javed, Y., Salehin, K. M. & Shehab, M. (2020). A study of South Asian websites on privacy compliance. *IEEE Access,* 8, 156067-156083. https://doi.org/10.1109/ACCESS.2020.3019334

Kautto, T. & Henttonen, P. (2017). Availability and findability of FOI and privacy statements on Finnish municipalities' websites. *Tidsskriftet Arkiv,* 8(1). https://doi.org/10.7577/ta.1968

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications. https://doi.org/10.4135/9781071878781

Kumar, N. & Verma, S. (2018). Content analysis of library websites of NAAC-accredited 'A' grade university in the central zone of India: A study. *Library Waves,* 4(2), 68-77. Retrieved from https://www.librarywaves.com/index.php/lw/article/view/69/71

Lin, X., Liu, H., Li, Z., Xiong, G. & Gou, G. (2022). Privacy protection of China's top websites: A multi-layer privacy measurement via network behaviors and privacy policies. *Computers & Security,* 114, 102606. https://doi.org/10.1016/j.cose.2022.102606

Lund, B. D. (2021). Public libraries' data privacy policies: A content and cluster analysis. *The Serials Librarian,* 81(1), 99-107. https://doi.org/10.1080/0361526X.2021.1875958

MAMPU. (2015). *Dasar privasi dan keselamatan ialah dasar agensi dalam mengurus, melindungi dan mengedar maklumat yang sensitif.* Retrieved from https://www.pnm.gov.my/pnm/resources/pdf%20file/dasar/PKPA_Bil._2_2015_-_Pengurusan_Laman_Web_Agensi_Sektor_Awam_(1)_.pdf [in Malay]

Mohan, J., Wasserman, M. & Chidambaram, V. (2019). Analyzing GDPR compliance through the lens of privacy policy. In *Heterogeneous data management, polystores, and analytics for healthcare: VLDB 2019 workshops* (pp. 82–95). Springer International Publishing. https://doi.org/10.1007/978-3-030-33752-0_6

Mukherjee, S. & Gutierrez, J. (2024). An examination of industry privacy statements in top New Zealand websites. In *Proceedings of the International Conference on Information Resources Management (CONF-IRM 2024).* https://aisel.aisnet.org/confirm2024/18/

Narimene, A. Z. & Mehdi, K. M. A. (2024). Algerian e-commerce firms' collection and usage of customers' personal data: An exploratory study. *Finance & Business Economies Review,* 8(3), 43-55. https://doi.org/10.58205/fber.v8i3.1853

Ong, R. (2023). Mandatory data breach notification: Its role in protecting personal data. *Journal of International and Comparative Law,* 10(1), 87-111. Retrieved from https://www.jicl.org.uk/storage/journals/June2023/J1fjQwq0kHkl3Q6Yb2Fy.pdf

Panda, S. & Kaur, N. (2023). Enhancing user experience and accessibility in digital libraries through emerging technologies. In K. P. Sinhamahapatra et al. (Eds.), *Digital libraries: Sustainable development in education* (pp. 676–703). https://doi.org/10.5281/zenodo.10211088

Reddick, C. G. & Zheng, Y. (2018). Online privacy protection in chinese city governments: An analysis of privacy statements. In: Alcaide Muñoz, L., Rodríguez Bolívar, M. (Eds) *International E-Government Development* (pp. 99-120). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-63284-1_5

Shah, M. A. H. & Hossain, M. S. (2022). Evaluation of public university libraries' websites in Bangladesh: Features, contents, and maintenance issues. *Journal of Information Management and Practices,* 2(1), 18-40. https://doi.org/10.52461/jimp.v2i1.1024

Shreiner, B. (2023). *The nuances of privacy policies within three types of archival institutions*. Master's paper. University of North Carolina at Chapel Hill, School of Information and Library Science. https://doi.org/10.17615/mn7c-0020

Šidlauskas, A. (2021). The role and significance of the data protection officer in the organization. *Socialiniai Tyrimai*, 44(1), 8-28. https://doi.org/10.15388/Soctyr.44.1.1

Solove, D. J. (2022). The limitations of privacy rights. *Notre Dame Law Review,* 98, 975-1020. Retrieved from https://scholarship.law.nd.edu/ndlr/vol98/iss3/1

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S. & Serna, J. (2018). PrivacyGuide: Towards an implementation of the EU GDPR on internet privacy policy evaluation. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics* (pp. 15–21). https://doi.org/10.1145/3180445.3180447

Valentine, G. & Barron, K. (2022). An examination of academic library privacy policy compliance with professional guidelines. *Evidence-Based Library and Information Practice,* 17(3), 77-96. https://doi.org/10.18438/eblip30122

Vanezi, E., Zampa, G., Mettouris, C., Yeratziotis, A. & Papadopoulos, G. A. (2021, May). Complicy: Evaluating the GDPR alignment of privacy policies-a study on web platforms. In *International Conference on Research Challenges in Information Science* (pp. 152-168). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-75018-3_10

Vaughan, J. (2020). Data security, integrity, and retention. *Library Technology Reports,* 56(6), 36-45. Retrieved from https://journals.ala.org/index.php/ltr/article/view/7408/10215

Vos, M., Hu, M. & Du, B. (2020). Privacy on Facebook brand pages: A content analysis study of New Zealand organizations. *ACIS 2020 Proceedings,* 53. Retrieved from https://aisel.aisnet.org/acis2020/53

Wang, J. (2022). Personalized information service system of smart library based on multimedia network technology. *Computational Intelligence and Neuroscience,* 2022, 2856574. https://doi.org/10.1155/2022/2856574