International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.529

Assessing the Alignment of Automotive Privacy Practices with Malaysia's PDPA

Nur Shahirah Hafizah Mohd Shani, Hafizah Mansor
Department of Computer Science, Kuliyyah of ICT, International Islamic University Malaysia

*Corresponding author hafizahmansor@iium.edu.my
(Received: 24th December 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract— Every day, the technology around us rapidly develops, and we see a global shift in the car industry. Despite the growth of car technology, we can see many data breaches in the car ownership life cycle. In one research by Mozilla, 84% of car brands surveyed reserve the right to share user data with third-party companies, and 76% can sell it. It has drawn a lot of attention in the car privacy industry as customers should have control over their data and privacy because of the different sensitivity levels of this data. In Malaysia, any connected device that handles personal data is subject to the Personal Data Protection Act 2010 (PDPA) which is an act that regulates the processing of personal data regarding commercial transactions. This study evaluates the compliance of automotive privacy policies with Malaysia's Personal Data Protection Act (PDPA), focusing on the privacy policies of Honda, Perodua, BMW, Nissan, Toyota, and Tesla. As connected car technologies become more prevalent, concerns regarding data privacy have intensified, necessitating strict adherence to privacy regulations. The study analyses these brands' privacy policies by extracting and evaluating keywords related to PDPA principles, such as data processing, security, retention, and data subject rights using Python keyword extraction. The extracted keywords are then used in the manual analysis for each privacy policy across PDPA. Findings reveal varying levels of compliance: Toyota emerges as the most compliant brand with a score of 2.571 out of 3, followed by Tesla at 2.285, indicating relatively high adherence to PDPA requirements. In contrast, Perodua shows the lowest compliance score at 1.428, highlighting critical gaps in data retention, security, and access principles. BMW, Honda, and Nissan demonstrate moderate compliance, scoring 1.857, 1.714, and 1.571, respectively. These results suggest that while some brands have made progress in aligning with PDPA principles, significant gaps remain in key areas, particularly in security, retention, and access, indicating a need for substantial policy revisions to improve data protection in the automotive sector.

Keywords— Automotive, PDPA, GDPR, Privacy Policy, Keywords, Compliance

I. INTRODUCTION

The rapid advancement of vehicle technologies, including connected cars and the Internet of Things (IoT), has transformed the automotive industry into a data-driven ecosystem. Modern vehicles now collect extensive personal and environmental data, raising significant privacy concerns. As car manufacturers adopt data-intensive technologies, ensuring the protection of user data has become a critical issue in the industry [1].

Despite claims of compliance with data privacy regulations, many car manufacturers fail to implement robust privacy measures. According to a report by the Mozilla Foundation, the automotive industry ranks as "the official worst category of products for privacy" ever reviewed, with most car brands drafting privacy policies but failing to enforce them effectively [2]. Data breaches affecting sensitive customer information are frequently reported, further exposing the vulnerabilities in current automotive privacy frameworks. Moreover, vehicle manufacturers often provide limited options for users to control how their personal data is collected, shared, and used.

From a consumer perspective, the level of engagement with privacy policies remains low. A survey conducted by the Pew Research Center found that only 9% of Americans consistently read privacy policies before agreeing to them, reflecting a widespread lack of awareness and understanding of privacy terms [3]. This passive acceptance raises critical questions about whether privacy policies in the automotive industry are truly effective or merely symbolic. Many consumers unknowingly provide blanket consent to data collection practices, leaving them vulnerable to unauthorised data use and privacy violations. This lack of transparency and awareness weakens consumer trust in automotive companies and the data protection frameworks that safeguard their privacy.

The compliance of automotive privacy policies also has broader societal implications. Privacy policies that are poorly implemented or inadequately enforced can lead to increased risks of data misuse, unauthorised sharing, and

exposure to cyber threats. Conversely, robust privacy practices promote accountability, transparency, and trust, benefiting both consumers and society by reducing the risk of data breaches and ensuring that personal data is handled responsibly. Therefore, effective privacy compliance is crucial for fostering ethical data practices in the automotive industry.

Failing to comply with privacy regulations poses significant risks to car companies and users. For automotive companies, non-compliance can result in legal penalties, loss of customer trust, and damage to brand reputation. The financial consequences of regulatory fines under privacy laws such as the General Data Protection Regulation (GDPR) or the Personal Data Protection Act (PDPA) can be substantial. Furthermore, users are exposed to privacy risks such as unauthorised data access, identity theft, and loss of control over their personal information. Inadequate privacy practices can undermine consumer confidence in connected vehicles, affecting user adoption of new technologies and impacting the industry's growth.

However, compliance alone does not guarantee that privacy policies are properly enforced or implemented. There is a critical distinction between compliance, enforcement, and implementation in the context of privacy practices. While a company may formally comply with privacy laws by drafting privacy policies and including the necessary terms, enforcement mechanisms are often weak, and the actual implementation of privacy practices varies widely across companies. For instance, a company may claim compliance by providing users with privacy policies but fail to actively protect user data or address potential security vulnerabilities. This gap between compliance on paper and real-world enforcement remains a major challenge in ensuring data privacy in the automotive sector.

Therefore, for privacy policies to be effective, compliance must go beyond documentation to include meaningful enforcement and operational implementation of data protection measures. Companies must ensure that privacy frameworks are not merely symbolic but are actively monitored, audited, and enforced across all levels of operations. Without this, even companies that comply with privacy regulations may expose users to privacy risks due to inconsistent enforcement and incomplete implementation.

To address these privacy concerns, various legal acts and frameworks have been established worldwide. The European Union's GDPR has set a global standard for data privacy governance. Similarly, countries such as Japan, the United States, and Malaysia have enacted their own privacy laws, including Japan's Act on the Protection of Personal Information (APPI), California's Consumer Privacy Act (CCPA), and Malaysia's PDPA. These regulations provide legal guidance for organisations to structure and implement privacy policies that align with internationally recognised principles [4].

Despite the presence of such regulations, many automotive companies still struggle to apply privacy principles effectively. This study focuses on assessing the compliance of privacy policies from six prominent car brands (Honda, Perodua, BMW, Nissan, Toyota, and Tesla) against the seven core principles outlined in Malaysia's PDPA - i. General Principle, ii. Notice and Choice Principle, iii. Disclosure Principle, iv. Security Principle, v. Retention Principle, vi. Data Integrity Principle and vii. Access Principle. The research involves keyword extraction and policy evaluation to determine the extent of compliance and identify gaps between regulatory expectations and actual implementation.

The contribution of this study is both practical and academic. This study provides actionable insights for automotive companies to strengthen their privacy policies and improve compliance practices. This study aims to develop a comprehensive privacy compliance evaluation framework tailored specifically to the automotive sector.

The two research questions for this study are: 1. How well do automotive privacy policies align with the seven principles of Malaysia's PDPA? and 2. What gaps exist between current privacy policies and legal requirements as specified by the PDPA?

By addressing these questions, this research seeks to enhance data privacy practices in the automotive industry while promoting greater transparency and user understanding of privacy policies.

II. RELATED WORKS

The rapid growth of connected vehicles has brought significant privacy concerns due to the massive amounts of personal data car manufacturers collect. As connected vehicles gather vast amounts of sensitive data - ranging from GPS location to driving behaviour - privacy issues related to transparency, user control, and data security have emerged as major challenges. Many automotive companies lack clarity in disclosing data collection practices, and users are often provided with limited control over their personal information [5]. Furthermore, these concerns raise important questions regarding compliance with privacy acts and regulations, as automotive companies may face significant challenges in securing personal data, particularly in the face of frequent vulnerabilities in vehicle data-sharing platforms [7]. However, it is crucial for both manufacturers and users to recognise the importance of data protection. Users must be educated on the extent of personal data shared by vehicles and be empowered to make informed decisions regarding their consent [8], [20].

Connected vehicles, designed to enhance user experience through real-time data sharing, raise substantial privacy issues. The sheer volume of personal data collected, such as geolocation, driving behaviour, and vehicle status, requires manufacturers to implement stringent data protection measures. The lack of transparency regarding data collection practices is a significant challenge in the automotive industry. Many companies fail to fully disclose how data is used, where it is stored, and who has access to it, making it difficult for consumers to understand the implications of their data being collected. Furthermore, limited user control over their personal information, including the ability to opt-out of data collection, exacerbates privacy concerns [5], [6]. With data breaches and cybersecurity risks on the rise, automotive companies face increasing pressure to ensure the privacy and security of personal data [7].

To address these privacy challenges, compliance with data protection regulations such as the GDPR and Malaysia's PDPA is essential. The GDPR provides a comprehensive framework for managing personal data in the European Union, establishing privacy rights and data security as fundamental principles [13]. The PDPA, enacted in Malaysia in 2010, serves as a legal framework for regulating personal data protection in commercial transactions, ensuring that data controllers and processors meet specific requirements for data collection, processing, and retention [19].

However, many automotive companies struggle to create clear, enforceable privacy policies that comply with these regulations. A study by Smit indicates that before and after the enforcement of the GDPR, privacy policies in the automotive sector showed significant improvements in terms of transparency and user consent. These regulations emphasise the importance of obtaining informed consent for sensitive data, such as geolocation and driving behaviour. As a result, it is imperative for manufacturers to update their privacy policies to align with these legal standards and ensure better user transparency [9], [10]. The role of consent, data security, and the right to be forgotten is central to both the GDPR and PDPA, but enforcement remains inconsistent, particularly in regions like Malaysia, where many organisations face compliance challenges [12], [19].

The GDPR and PDPA are critical in ensuring that personal data is protected throughout its lifecycle, particularly in industries like automotive, where data collection is extensive. The GDPR's two main pillars—privacy rights and data security—are designed to ensure that individuals' personal data is handled ethically and securely. For instance, the regulation mandates businesses to seek explicit consent before collecting sensitive information and grants individuals the right to access, rectify, or delete their personal data [13].

The PDPA, similarly, regulates personal data collection and processing in Malaysia, focusing on principles such as Notice and Choice, Security, Retention, and Data Integrity. Despite its comprehensive structure, PDPA enforcement has been limited, and many businesses, including those in the automotive industry, have struggled with consistent implementation [19]. This challenge is highlighted by studies that reveal organisations often fail to define clear data collection and retention policies, leading to potential non-compliance with the Act [12]. Furthermore, while the GDPR has inspired similar privacy rules in various countries, such as Chile, Brazil, and Japan, the automotive industry must still adapt its practices to ensure compliance with local data protection laws like PDPA, especially when operating across international borders [13], [19].

Despite the comprehensive nature of both the GDPR and PDPA, many organisations, particularly in the automotive industry, face significant challenges in complying with these regulations. Key areas of difficulty include consent management, data portability, and ensuring the right to be forgotten. These provisions are difficult to implement due to the complexities of managing vast amounts of data collected from connected vehicles. In Malaysia, businesses often face challenges translating these regulatory requirements into actionable policies that are aligned with the PDPA. For example, obtaining user consent for data collection in connected vehicles requires clear communication of what data is being collected and how it will be used. Similarly, ensuring data portability and facilitating the right to be forgotten in the context of highly interconnected vehicle data systems presents considerable obstacles. The automotive sector, with its data-intensive technologies, must address these challenges to ensure full compliance with both GDPR and PDPA regulations [17].

To assess compliance with privacy regulations, methodologies such as keyword extraction have proven invaluable in evaluating the contents of privacy policies. By identifying and analysing relevant keywords, researchers can automate the process of determining whether a privacy policy aligns with the principles of data protection laws like GDPR and PDPA [14], [15]. Keyword extraction techniques are particularly useful in evaluating large datasets of privacy policies, enabling more efficient and comprehensive analysis of how automotive companies adhere to privacy regulations [16].

A framework using keyword-based methods for privacy policy enforcement in connected automotive systems has been proposed to enhance the compliance process [14], [15]. This framework can be applied to assess how automotive companies handle data collection, security,

retention, and user consent, ensuring they meet the regulatory requirements set forth by laws such as the GDPR and PDPA. Moreover, studies such as McDonald's comparative policy analysis also provide foundational methods for analysing privacy policies and improving compliance evaluation [16]. In other paper, by Das Chaudhury and Choe further highlight that the adoption of regulatory regulation like the GDPR requires organizations to implement systematic compliance mechanisms, such as privacy-by-design approaches, to ensure that privacy safeguards are embedded throughout data processing activities [18].

The intersection of connected vehicles, privacy regulations, and data protection presents a complex landscape for the automotive industry. While regulations like the GDPR and PDPA provide robust frameworks for protecting consumer data, challenges in enforcement and compliance persist, particularly in the automotive sector. This literature review highlights the importance of data protection regulations and the growing need for automotive companies to ensure compliance with both local and international data privacy laws [13], [19].

Despite the existing frameworks, there are significant gaps in the enforcement of these regulations, particularly in countries like Malaysia where the PDPA faces implementation challenges. The literature also suggests that innovative methodologies, such as keyword extraction, can be instrumental in assessing privacy policy compliance. By addressing these research gaps and applying advanced methods to evaluate compliance, this study aims to contribute both practical and theoretical insights into improving data privacy practices in the automotive industry, ultimately helping to bridge the enforcement gaps in privacy policy compliance [10], [12], [13], [14].

III. METHODOLOGY

A. RESEARCH DESIGN

The study follows a qualitative content analysis framework, focusing on the textual evaluation of automotive privacy policies. This design is chosen because privacy policies are inherently text-based legal documents. The research assesses compliance by matching policy content against pre-defined PDPA criteria using both automated and manual methods. This dual approach ensures accuracy and context-aware analysis.

B. DATA COLLECTION

The study focuses on six major car brands: Perodua, BMW, Tesla, Nissan, Toyota, and Honda, selected based on their industry significance, market reach, and relevance to data privacy concerns. Perodua, Malaysia's top-selling local car brand, provides a crucial perspective on compliance with the Malaysian Personal Data Protection Act (PDPA). BMW enables an analysis of how global automotive brands adapt their privacy policies to meet international data protection standards. Similarly, Toyota recognised as the world's best-selling car brand with record-breaking sales in September 2024, was selected to explore how a globally dominant automotive manufacturer ensures privacy compliance across multiple jurisdictions. Tesla earned its place due to its notable privacy controversies, including being flagged by the Mozilla Foundation for poor privacy practices and untrustworthy Artificial Intelligence (AI) implementations. This makes Tesla an important case for understanding privacy risks in AI-powered connected vehicles. Nissan was chosen because of its reputation for collecting some of the most intrusive categories of personal data, such as "sexual activity," raising serious concerns about excessive data collection practices. Honda, positioned as a mid-tier performer in privacy assessments, provides a balanced perspective, bridging the gap between brands with strong privacy policies and those facing significant privacy challenges.

To collect and extract privacy policies from these car brands, the study employed web scraping using the BeautifulSoup library in Python. This method automated the retrieval of publicly available privacy policy text from the official websites of the selected brands. The process involved sending web requests using the "request" library and parsing the HTML content using BeautifulSoup for efficient text extraction.

However, for Tesla and Toyota, there is a restriction to directly retrieve the policies. Hence, we manually copied it from the official website and saved it into PDF and we read the PDF and extracted the keywords using Python.

C. DATA PRE-PROCESSING

Data pre-processing involved automated and manual methods to ensure the collected privacy policies were clean, standardised, and ready for analysis. This two-fold approach maximised accuracy and minimised noise in the data, enabling precise evaluation of compliance with data privacy regulations.

In pre-processing, we performed web scraping, text processing, and data analysis to assess the compliance of all car brands' privacy policies with Malaysia's PDPA. It starts by importing essential libraries: "requests" for fetching web content, "BeautifulSoup" for parsing HTML, "re" for text cleaning and pattern matching, "pandas" for data organisation, and "matplotlib.pyplot" for visualisation.

We fetched the privacy policy webpage of the selected car brands using requests.get() and checked if the retrieval was successful. If successful, then "BeautifulSoup" was used to parse the page's HTML content, extracting the relevant privacy policy section based on a specified HTML

https://doi.org/10.31436/ijpcc.v11i1.529

tag and class. If the section is found, the text is cleaned using a function that preserves key phrases, removes special characters, and standardises the text to lowercase.

We used the clean_text() function that prepares the privacy policy text for keyword matching by standardising its format. It starts by defining a list of important multi-word phrases like "up-to-date," "unauthorised access," and "correct personal data" to preserve them during text cleaning. To prevent these phrases from being split, it temporarily replaces spaces within them with underscores. The function then removes excess whitespace using a regular expression that condenses multiple spaces, tabs, or newlines into a single space. It also removes special characters, punctuation, and symbols while keeping only letters, numbers, underscores, and spaces. After cleaning, the function restores the preserved phrases by replacing underscores with spaces. Finally, it converts the entire text to lowercase, ensuring case-insensitive keyword matching. This process standardises the text, making it easier to search for relevant terms accurately.

D. DATA ANALYSIS

1) Automated Data Analysis

Following text cleaning in Section C, the system uses a Python function, count_keywords, to identify and count occurrences of the defined keywords. The function operates by scanning the cleaned text for exact matches of each keyword using regular expressions. It ensures that only whole-word matches are detected, avoiding partial or unintended matches, and tracks the keywords found in a list of unique matches.

The keyword counts are then analysed to determine compliance with each PDPA principle. A compliance percentage is calculated by comparing the number of matched keywords against the total number of keywords defined for a given principle (see Table 1).

TABLE I
SCORING TABLE

Range	Score	Compliance Level	Description
75% - 100%	3	High Compliance	Most or all relevant keywords are present
50% - 74%	2	Moderate Compliance	Partial Coverage
1% - 49%	1	Low Compliance	Limited references
0%	0	Non-Compliance	No relevant keywords found

This percentage quantifies the degree of alignment between the policy and PDPA requirements. Based on the calculated percentages, compliance levels are assigned using predefined thresholds: High Compliance (75%-100%), Moderate Compliance (50%-74%), Low Compliance (1%-49%), or Non-Compliance (0%) as stated in Table 1. Compliance scores are then calculated using a standard percentage formula: Compliance Score=Number of Keywords/Sum of Keyword Matches×100 This formula evaluates how well the policy aligns with each PDPA principle. Our formula assesses compliance by calculating the proportion of matched keywords for each principle, serving as a proxy for the presence of required provisions [21], [22]. If all relevant keywords are present, the principle receives a 100% compliance score. If some keywords are missing, the score reflects partial compliance based on the proportion of matched keywords. The scoring level is shown in Table 1.

This automated process provides a fast and objective assessment of the privacy policy's coverage of PDPA principles. However, it cannot interpret the context or accuracy of keyword usage, limiting its ability to fully evaluate compliance. As a result, a manual review is conducted to complement the automated findings, ensuring a thorough and context-aware analysis.

Next, to calculate the overall compliance, we take the level of compliance for each principle and compute the average:

Overall Compliance Level = ∑Compliance Levels/Number of Principles

This formula is used because averaging the compliance levels gives a single metric that summarises how well an organisation adheres to the principles outlined in privacy policies. This approach is valuable because it simplifies complex compliance assessments into a single, interpretable figure that reflects the organisation's overall adherence to privacy standards across multiple dimensions [23].

2) Manual Data Analysis

Due to the inability of automation to interpret context, a manual review was conducted to ensure a comprehensive and accurate assessment of compliance with the PDPA. This manual process began with an in-depth examination of the privacy policy for each car brand. For each matched keyword identified during the automated analysis, its context within the policy was carefully reviewed to determine alignment with the specific requirements and intent of the PDPA principles.

Further analysis was performed to identify synonyms or alternative expressions of missing keywords. This included checking for variations in grammatical forms, such as past or present tense, noun forms, or other terminology that may convey the same meaning as the original PDPA keywords. By analysing these linguistic variations, the review accounted

https://doi.org/10.31436/ijpcc.v11i1.529

for any differences in language that may still reflect compliance with PDPA standards.

Additionally, the entire privacy policy was thoroughly re-read to evaluate its overall structure, language, and alignment with PDPA principles. This holistic review ensured that the provisions in the policy collectively adhered to the regulatory framework, even if certain keywords were not explicitly present.

Compliance scoring was manually updated using the same scoring in Table 1 to reflect the findings from the contextual review. These manual adjustments provided a refined and accurate evaluation of the privacy policy's adherence to PDPA principles, addressing limitations in the automated methodology and ensuring a robust assessment of compliance.

IV. RESULTS AND FINDINGS

The findings indicate that the car privacy policy demonstrates moderate compliance, with notable strengths in data collection but room for improvement in areas such as data retention and security. Perodua, shows consistent compliance, particularly in data access and integrity, although greater transparency in data processing and third-party disclosures is needed. BMW exhibited high compliance, particularly in data security and retention practices, aligning well with PDPA requirements. In contrast, Nissan exhibited moderate to low compliance, particularly in areas related to data subject rights and third-party disclosures, highlighting potential vulnerabilities. Toyota displayed moderate compliance, with strengths in data collection and security but areas for improvement in retention and data integrity. Finally, Tesla demonstrated high compliance overall, excelling in data security and access, although gaps in data retention and third-party disclosures were observed.

A comprehensive set of keywords for each PDPA principle is defined. These keywords were derived by thoroughly studying the PDPA, consulting legal websites, and analysing privacy resources to ensure their alignment with the principles' intent. For example, the "General Principle" includes keywords like "processing," "personal data," and "consent," while the "Security Principle" focuses on terms such as "data protection," "unauthorised access," and "security measures." These keywords encapsulate the essential aspects of each principle, forming the backbone of the automated compliance evaluation. Table 2 defines all the keywords considered.

Next, in the case of Honda brand, the automated analysis for the General Principle showed a match of 3 out of 6 keywords, resulting in a compliance score of 50% and an initial score of 2. Upon manual review, it was observed that the missing keyword "sensitive personal data" was indirectly addressed in the policy under the section detailing the types of data being processed. This implied compliance with the General Principle's intent, leading to an adjustment in the score from 2 to 3, as documented in Table 3.

Similarly, for Perodua, the automated analysis identified two matched keywords—"data protection" and "protect"—under the Security Principle. However, manual analysis revealed that these terms were not used in the context of data security measures as required by the PDPA. Furthermore, a detailed review of the privacy policy found no mention of security principles. Consequently, the compliance level was adjusted from 1 to 0, as noted in Table 4.

The same methodology was applied across the privacy policies of other car brands. Each principle was carefully scrutinised to ensure that the context of matched keywords aligned with PDPA requirements, and any indirect or implied compliance was accounted for. Missing or irrelevant keywords were also verified to prevent overestimation of compliance. These adjustments provided a more accurate and nuanced evaluation of each brand's adherence to PDPA principles. The details of other adjustments can be referred to in Table 5 to Table 8 for BMW, Nissan, Toyota and Tesla respectively.

The findings reveal considerable variability in compliance levels, indicating partial alignment with the PDPA. Toyota demonstrated the highest overall compliance, with strong performance across principles such as Notice and Choice, Disclosure, Security, and Access. Tesla followed closely, with similar strengths but notable weaknesses in Retention and Data Integrity. Honda, BMW, Nissan, and Perodua showed lower levels of compliance overall, with significant deficiencies in Security, Retention, and Access, highlighting critical vulnerabilities. Figures 1 to 6 present the analysis for each car brand. Figure 7 shows the chart for each car brand across the compliance for each principle.

Fig. 1: Honda privacy compliance across PDPA

https://doi.org/10.31436/ijpcc.v11i1.529

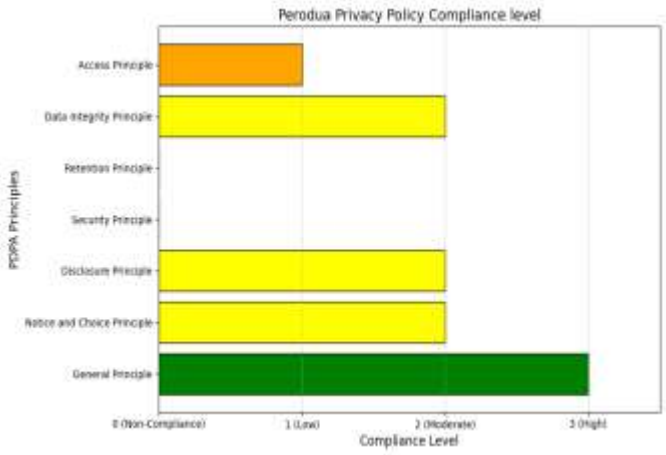

Fig. 2: Perodua privacy compliance across PDPA

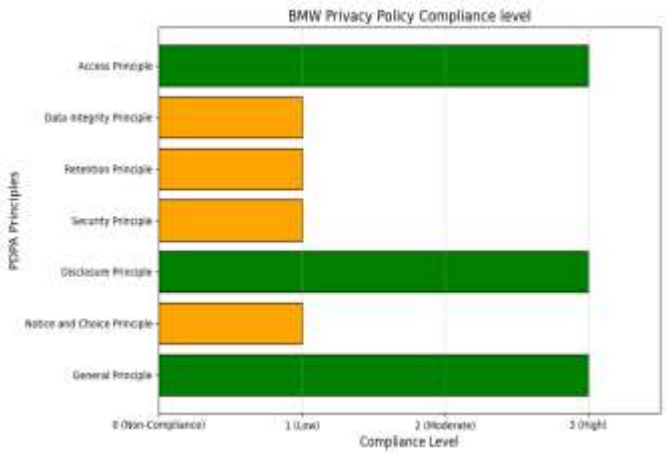

Fig. 3: BMW privacy compliance across PDPA

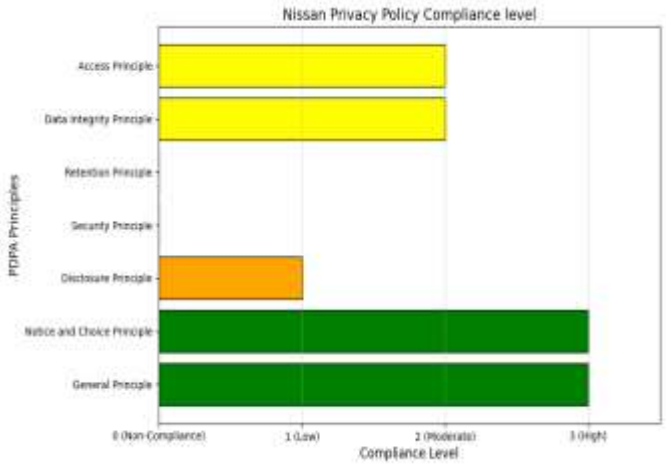

Fig. 4: Nissan privacy compliance across PDPA

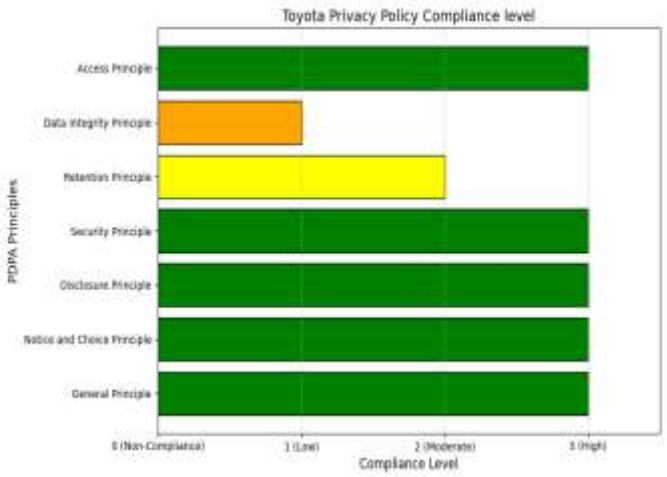

Fig. 5: Toyota privacy compliance across PDPA

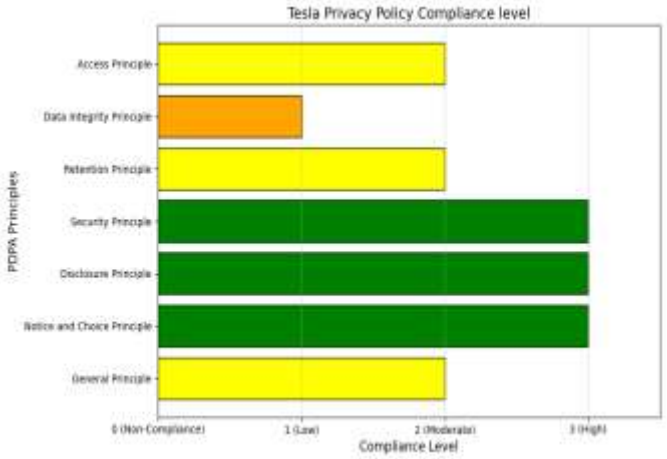

Fig. 6: Tesla privacy compliance across PDPA

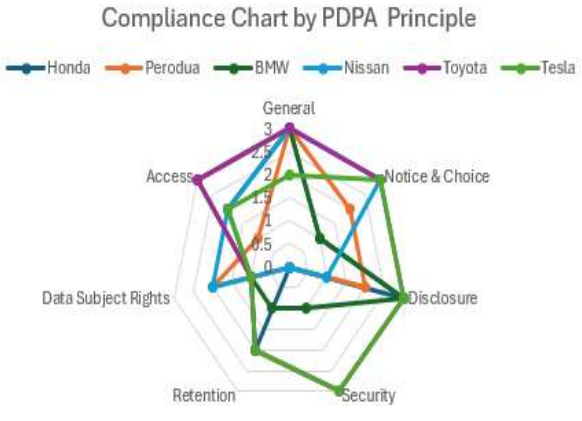

Fig. 7: Compliance chart by PDPA Principle

https://doi.org/10.31436/ijpcc.v11i1.529

The analysis shows that most brands achieve moderate compliance with General, Notice and Choice, and Disclosure, showing efforts to inform users about data collection, processing purposes, and third-party relationships. However, principles like Security, Retention, and Data Integrity were poorly addressed across all brands except Toyota and Tesla, which provided some details on security measures and data retention. In contrast, brands like Perodua and Nissan failed to mention security practices, and most brands lacked clear policies on data retention timelines and deletion protocols.

The results answer the study's research questions by demonstrating that the automotive brands' privacy policies align only partially with the seven principles of the PDPA. Significant gaps exist in areas critical to data protection, such as Security, Retention, and Data Integrity. These gaps indicate an urgent need for automotive companies to enhance their privacy policies to ensure full compliance with PDPA requirements. The findings suggest that while progress has been made in areas like Notice and Choice, and Disclosure, there is still much work needed to address deficiencies in Security and Retention, which are essential for safeguarding personal data. The study underscores the importance of a comprehensive and uniform approach to privacy policy development within the automotive industry.

Looking at the data in Figure 8, Toyota emerges as the most compliant car manufacturer, with an overall compliance score of 2.571, indicating that it is better aligned with the privacy principles compared to others. Tesla follows with a score of 2.285, suggesting a relatively high level of compliance. On the other end, Perodua shows the lowest compliance level with a score of 1.428, highlighting areas for improvement in its privacy practices. Other companies like BMW (1.857), Honda (1.714), and Nissan (1.571) display varying levels of compliance.

The overall results conclude that most of the brands studied do not fully comply with the PDPA, and there is a clear need for revisions to their privacy policies. These revisions should focus on improving transparency, ensuring data retention practices align with legal requirements, and addressing the rights of data subjects, to better protect consumer privacy and align with Malaysia's data protection laws. For compliance to be effective, it must go beyond documentation to enforcement and practical implementation, ensuring that users' personal data is genuinely protected. Only by bridging this gap can the automotive industry achieve meaningful and lasting improvements in data privacy practices.

Nonetheless, the compliance evaluation framework developed in this study is adaptable and can serve as a baseline for assessing other car brands' privacy policies. The keyword extraction method and PDPA principles used in this analysis offer a scalable approach to measuring privacy policy compliance across the automotive industry. However, differences in legal environments, data collection practices, and enforcement mechanisms must be considered when applying these results to other brands.

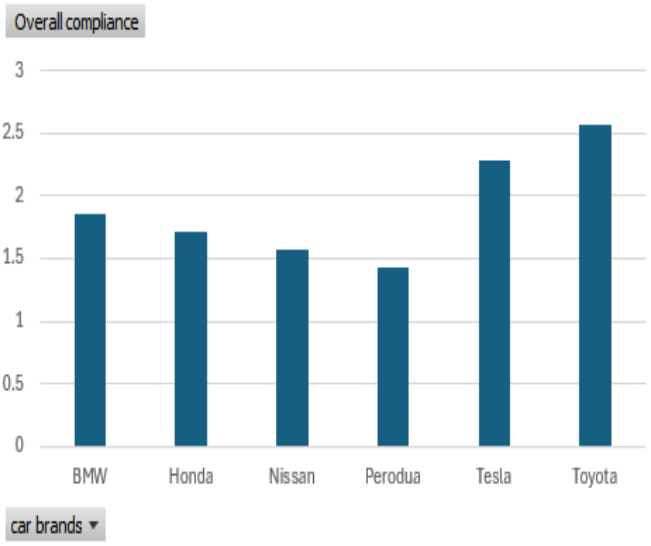

Fig.8 Overall compliance across PDPA

However, it is important to highlight that compliance does not always translate into effective enforcement and implementation. While companies may draft privacy policies that formally meet regulatory requirements, these policies must be enforced through proper governance mechanisms and implemented in practice. The gap between compliance, enforcement, and implementation varies across companies, meaning that even if a company claims compliance, the actual measures taken to protect user data may be insufficient. For instance, a privacy policy may mention security practices, but without clear enforcement or practical implementation, users remain vulnerable to data breaches and misuse. Therefore, compliance on paper alone is not enough to guarantee robust data protection.

The impact of non-compliance can be severe for both car manufacturers and consumers. For car companies, failing to comply with privacy laws can result in financial penalties, loss of customer trust, and reputational damage. Data breaches and poor privacy practices may also deter consumers from adopting connected car technologies, ultimately affecting the company's growth and market position. For consumers, non-compliance increases the risk of unauthorised data use, identity theft, and privacy violations, leading to diminished control over personal information and potential harm.

Additionally, the study's findings raise the question of whether the results can be generalised to all car brands. While the research focused on six prominent car

manufacturers, the varying compliance levels observed suggest that the results may not apply uniformly across the entire automotive industry. Differences in compliance could be influenced by regional policies, corporate governance structures, and market priorities. Therefore, further research is needed to assess whether similar gaps exist in the privacy policies of other brands and different jurisdictions.

In conclusion, this study provides a repeatable methodology, but the results should be interpreted with caution when applied to other car manufacturers. Further analysis would be required to account for specific privacy practices and legal obligations applicable to different regions and brands.

V. LIMITATIONS AND FUTURE WORKS

A key limitation of this study is the reliance on publicly available privacy policies, which may not fully represent a company's actual practices. The analysis uses keyword matching, which may miss important nuances in the policies, leading to incomplete compliance assessments. The study also only includes a small number of automotive brands, so the findings may not apply to all manufacturers or regions.

There is a potential source of bias in this study that lies in the selection of keywords used to evaluate compliance with Malaysia's PDPA. The keywords were chosen based on the researcher's interpretation of the seven PDPA principles and the common language used in privacy policies. However, this process may have unintentionally excluded certain synonyms or phrases that could indicate compliance, leading to an underestimation of adherence. Similarly, over-reliance on specific keywords may cause an overestimation of compliance if policies use the right terminology without adequately implementing the corresponding privacy measures.

Bias also exists in the selection of car brands for the study. The research focused on six major car manufacturers — Toyota, Tesla, Honda, BMW, Nissan, and Perodua — chosen for their global presence and relevance in the Malaysian automotive market. While these brands provide valuable insights, the selection may not represent smaller or emerging car brands that could have different privacy practices. Additionally, the study primarily evaluated the English versions of privacy policies, which may introduce language-based bias and limit the generalisability of the results to brands that publish policies in other languages.

These biases impact the study by potentially affecting the accuracy of compliance scores and limiting the applicability of findings to other car brands. The keyword-based approach might not capture nuanced privacy practices, and the brand selection may overlook regional differences or variations in policy enforcement. Future studies should incorporate more comprehensive keyword sets, consider a wider range of car brands, and explore policies in multiple languages to enhance the generalisability of the findings.

Future research could broaden the analysis to include more automotive brands and regions, with a deeper review of policy language to assess true compliance. It could also explore the effects of low compliance on consumer trust and legal risks. Additionally, future studies could examine how companies update their policies in response to changing regulations and gather insights from experts to better understand compliance gaps. Using advanced keyword extraction methods like spaCy and KeyBERT could improve keyword identification accuracy, while stronger evaluation techniques could provide deeper insights into policy effectiveness.

ACKNOWLEDGEMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] A. Smith and B. Jones, "Data privacy challenges in the automotive industry: Navigating the era of connected vehicles," Journal of Automotive Technology and Ethics, vol. 15, no. 2, pp. 123–145, 2023.

[2] M. Jen, R. Misha, and M. Zoe, "It's official: Cars are terrible at privacy and security," Mozilla Foundation, 2023. [Online]. Available: https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

[3] G. A. Fowler, "Few read privacy policies. Would they if they were shorter?," The Washington Post, 2022. [Online]. Available: https://www.washingtonpost.com/business/2023/09/07/car-privacy-mozilla-report

[4] C. Brown, "Global data protection regulations and their impact on automotive data management," International Journal of Data Law, vol. 8, no. 1, pp. 78–102, 2022.

[5] C. Bodei et al., "Vehicle data collection: A privacy policy analysis and comparison," in International Conference on Information Systems Security and Privacy, 2023, pp. 626–633.

[6] G. Madzudzo, M. Cheah, and M. Kukova, "Data protection and connected vehicles: Privacy policy analysis from a consumer perspective," 2020. [Online]. Available: https://doi.org/10.13140/RG.2.2.28097.17769

[7] S. Prevost and H. Kettani, "On data privacy in modern personal vehicles," in ACM International Conference Proceeding Series, 2019. [Online]. Available: https://doi.org/10.1145/3372938.3372940

[8] G. Bella and P. Biondi, "Car drivers' privacy awareness and concerns," 2023. [Online]. Available: https://doi.org/10.13140/RG.2.2.14411.98080

[9] R. N. Zaeem and K. S. Barber, "The effect of the GDPR on privacy policies," ACM Transactions on Management Information Systems, vol. 12, no. 1, 2021. [Online]. Available: https://doi.org/10.1145/3389685

[10] F. Vallet, "The GDPR and its application in connected vehicles—Compliance and good practices," in Lecture Notes in Mobility. Springer Science and Business Media Deutschland GmbH, 2019, pp.

245–254. [Online]. Available: https://doi.org/10.1007/978-3-030-14156-1_21
[11] M. D. Pesé and K. G. Shin, "Survey of automotive privacy regulations and privacy-related attacks," SAE Technical Papers, vol. 2019-April, no. April, 2019. [Online]. Available: https://doi.org/10.4271/2019-01-0479
[12] S. Miskam et al., "Data privacy practices of private higher education institutions in Malaysia: A preliminary study," Journal of Information and Communication Technology, vol. 8, no. 2, 2023.
[13] I. Kara, M. Aydos, and A. Akca, "Privacy, security and legal aspects of autonomous vehicles," Çukurova Üniversitesi, 2020
[14] Z. H. Amur et al., "Unlocking the potential of keyword extraction: The need for access to high-quality datasets," 2023. [Online]. Available: https://doi.org/10.3390/app
[15] A. Bkakria, L. Brika, and L. A. Brika, "A framework for privacy policy enforcement for connected automotive systems," 2023.
[16] A. M. McDonald et al., "A comparative study of online privacy policies and formats," 2009.
[17] Ž. Spalević and K. Vićentijević, "GDPR and challenges of personal data protection," 2022.
[18] R. Das Chaudhury and C. Choe, "Digital privacy: GDPR and its lessons for Australia," Australian Economic Review, vol. 56, no. 2, pp. 204–220, 2023. [Online]. Available: https://doi.org/10.1111/1467-8462.12506
[19] A. Alibeigi and A. B. Munir, "Malaysian personal data protection act: A mysterious application," 2020.
[20] M. C. Gaeta, "Data protection and self-driving cars: The consent to the processing of personal data in compliance with GDPR," vol. 24, pp. 1–48, 2019.
[21] O. A. Cejas et al., "NLP-based automated compliance checking of data processing agreements against GDPR," IEEE Transactions on Software Engineering, vol. 49, no. 9, pp. 4282–4303, 2023. [Online]. Available: https://doi.org/10.1109/TSE.2023.3288901
[22] A. J. Aberkane, G. Poels, and S. vanden Broucke, "Exploring automated GDPR-compliance in requirements engineering: A systematic mapping study," IEEE Access, vol. 9, pp. 66542–66559, 2021 [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3076921
[23] J. Smith, Compliance in the Digital Age: Methods and Models. Compliance Press, 2020.

APPENDIX

TABLE II
DEFINITION AND KEYWORDS FOR EACH PRINCIPLE

Principle	Definition	Keywords
General	Personal data must be processed lawfully and fairly with consent for legitimate purposes.	processing, personal data, consent, sensitive personal data, lawful purpose, legal obligation
Notice and Choice	Data subjects must be informed of data collection, purpose, and rights, giving consent when needed	written notice, inform, right to access, third parties, third party, third party disclosure, access and correction, obligation, supply data, data subject rights, data processing, data collection purpose, data collection, data source, processed, on behalf of, request
Disclosure	Personal data must not be disclosed without consent unless required by law.	disclosure, without consent, data subject consent, third parties, purpose of disclosure, third party disclosure
Security	Reasonable security measures must be taken to protect personal data from risks like loss or misuse.	data protection, protect, security measures, unauthorised access, loss, misuse, modification, data storage location, secure transfer, data processor guarantees, guarantees
Retention	Personal data must not be kept longer than necessary for the purpose it was collected.	retention, deletion, destruction, data retention period, data deletion, purpose fulfillment, not be kept longer, permanently, destroyed
Data Integrity	Data must be accurate, complete, and up-to-date to avoid misleading information.	accuracy, accurate, complete, completeness, up-to-date, not misleading data
Access	Data subjects have the right to access and correct their personal data when necessary.	access to personal data, correct personal data, inaccuracy, data access right, data correction, access, correct, inaccurate, incomplete

https://doi.org/10.31436/ijpcc.v11i1.529

TABLE III
SUMMARY OF KEYWORD EXTRACTION FOR HONDA

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Giving extra details on processing "your personal data may be collected, processed and used for the following optional purposes"	3
Notice and Choice	1	Very little explanation of this principle	1
Disclosure	1	Explained clearly who is the third party even though the keyword is not found but it refers to the disclosure	3
Security	1	Does not mention anything regarding Security	0
Retention	0	Does not mention anything regarding retention	0
Data Integrity	0	Does mention complying with the Honda Data Integrity Policy	1
Access	1	Mentioned that "you may request for access to, correction, update"	2

TABLE IV
SUMMARY OF KEYWORD EXTRACTION FOR PERODUA

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	This notice explains how we collect and handle your personal data in accordance with the law even though the 'lawful' keywords are missing	3
Notice and Choice	1	Mentioned that "This written notice serves to inform you that your personal data is being processed by or on behalf of Perodua."	2
Disclosure	1	Personal data may be disclosed to the relevant third parties and it defines who are the third parties	2
Security	1	The 2 keywords matched do not refer to the Security principle	0
Retention	0	Does not mention anything regarding retention	0
Data Integrity	1	Mentioned ensuring that "the personal data you provide is accurate, complete and not misleading" and that such personal data is kept up to date	2
Access	1	Mentioned that "You may access and request for correction of your personal data". However there is only one line explanation and general.	1

https://doi.org/10.31436/ijpcc.v11i1.529

TABLE V
SUMMARY OF KEYWORD EXTRACTION FOR BMW

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Personal data are collected, processed and used for the business activities of BMW Group Malaysia but are not limited and also for optional purposes. They highlight all the purposes clearly.	3
Notice and Choice	1	All keywords matched are correct as per the context	1
Disclosure	1	Mentioned clearly that personal data may be disclosed to and processed by	3
Security	1	Mention little about the loss and security.	1
Retention	1	Mentioned deletion once but not detailed.	1
Data Integrity	0	Mentioned about the confidentiality and integrity of your personal data is a matter of prime importance	1
Access	1	Mentioned that "can request access to see any information stored about you and request correction, updating, or disabling of the same at any time"	3

TABLE VI
SUMMARY OF KEYWORD EXTRACTION FOR NISSAN

Principle /Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Mentioned clearly that "we are processing your personal data, including any additional information you may subsequently provide"	3
Notice and Choice	1	Mentioned that "This written notice serves to inform you that your personal data is being processed by or on behalf of ETCM". Also mentioned about purpose of personal data	3
Disclosure	1	Matched the keywords	1
Security	1	The keywords are not related to Security	0
Retention	0	Not mention anything regarding retention	0
Data Integrity	1	Mentioned that "You are responsible for ensuring that the personal data you provide us is accurate, complete and not misleading and that such personal data is kept up to date."	2
Access	1	Mentioned that "You may access and request for correction of your personal data and to contact us with any enquiries or complaints in respect of your personal data as follows in accordance with the PDPA:"	2

https://doi.org/10.31436/ijpcc.v11i1.529

TABLE VII
SUMMARY OF KEYWORD EXTRACTION FOR TOYOTA

Principle/Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Mentioned clearly what are the data collected and "given your consent for one or more specific purpose"	3
Notice and Choice	1	Mentioned clearly that "Your personal data is collected and further processed as required or permitted"	3
Disclosure	1	Mentioned clearly that "Your personal data provided to us may also be disclosed to the following classes of third parties." Define the third parties.	3
Security	1	Mentioned clearly that "UMWT takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of your personal data."	3
Retention	1	Mentioned that "The personal data collected shall be processed and stored for as long as required by the purpose they have been collected for. However, UMWT may be obliged to retain personal data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority." A full score is not possible due to a lack of clarity	2
Data Integrity	1	Just mentioned about accurate data	1
Access	1	Mentioned clearly that "You have the right to access, verify, update and correct your personal data held by us"	3

TABLE VII
SUMMARY OF KEYWORD EXTRACTION FOR TESLA

Principle/Items	Compliance level	Manual Adjustment reasons	Final Compliance level
General	2	Mentioned clearly but also states about Collection and Use of Non-Personal Data	2
Notice and Choice	1	Mentioned clearly this principle using other words with the same context as PDPA	3
Disclosure	1	Mentioned clearly this principle using other words with the same context as PDPA	3
Security	1	Mentioned clearly about "Security features to consistently protect your information. For example, your Tesla Account includes owner resources, guides and important documents, so we offer multi-factor authentication to protect your account"	3
Retention	1	Mentioned about retention. However, it does not clearly mention how long the data will be kept and is is based on the consideration of its use. Hence the scoring only increased to 2	2
Data Integrity	1	Matched the keywords	1
Access	1	Mentioned that "You can access your Tesla Account to update the information from or about you in that account at any time"	2