Democratizing GDPR Compliance: AI-Driven Privacy Policy Interpretation

Sangeeta Mittal*
Jaypee Institute of Information Technology
sangeeta.mittal@jiit.ac.in

Saksham Gupta
Jaypee Institute of Information Technology
guptasaksham2311@gmail.com

Kritarth Bansal
Jaypee Institute of Information Technology
bansalkritarth10@gmail.com

Geetali Aggarwal
Jaypee Institute of Information Technology
geetaliag02@gmail.com

ABSTRACT

With long privacy policies, users face the challenge of understanding them easily in order to ensure that their privacy rights are upheld. This paper presents an approach for democratizing GDPR compliance through AI-driven privacy policy interpretation. The methodology leverages advanced artificial intelligence techniques of Large Language Models (LLMs) for implementing effective comprehension of privacy policies. By extracting key information related to personally identifiable information (PII), the proposed solution empowers users to make informed decisions about their data privacy. The effectiveness of AI-driven privacy policy interpretation has been shown via various examples of automated summarization of lengthy and complex privacy policies as compliant/non-compliant to GDPR. Overall, it makes privacy policies more accessible, relevant, and actionable for users.

CCS CONCEPTS

• **Security and privacy** → Human and societal aspects of security and privacy; Privacy protections; • **Applied computing** → Law, social and behavioral sciences.

KEYWORDS

GDPR, LLMs, Personally Identifiable Information, Privacy

ACM Reference Format:
Sangeeta Mittal, Saksham Gupta, Kritarth Bansal, and Geetali Aggarwal. 2024. Democratizing GDPR Compliance: AI-Driven Privacy Policy Interpretation. In *2024 Sixteenth International Conference on Contemporary Computing (IC3-2024) (IC3 2024), August 08–10, 2024, Noida, India.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3675888.3676142

1 INTRODUCTION

In today's digital age, the proliferation of online platforms, applications, and digital services has revolutionized the way we interact with information. However, amidst this convenience lies a significant concern of our vulnerability to the compromise of personal data. The digital landscape, while offering immense opportunities, also exposes individuals to unprecedented risks regarding the privacy and security of their sensitive information. The core challenge revolves around the protection of individual privacy in this digital sphere. Our personal data is routinely collected, stored, and shared without complete transparency or explicit consent [1]. This lack of control over our own information leads to a loss of trust and raises substantial concerns about the misuse or unauthorized access to our data.

In the digital realm, lengthy and complex privacy policies on websites pose challenges for users in understanding the handling of their personally identifiable information (PII) and compliance with global privacy laws like General Data Protection Regulation (GDPR) [2]. GDPR has been enforced by governments to protect privacy rights of the individuals while using online services and force the organizations to collect and use users' data in responsible manner. The GDPR mandates that personal data is maintained safely by the collectors and be protected against "unauthorized or unlawful processing. A significant percentage of users often overlook or do not fully comprehend the content within privacy policies and cookie consent agreements [3]. This lack of empirical understanding of user behavior contributes to a substantial gap between users' expectations of data privacy and the actual use and sharing of their information by online platforms.

Moreover, empirical research has highlighted that despite the availability of privacy policies, users tend to grant consent without fully comprehending the implications. This insight raises concerns about informed consent and the actual protection of sensitive personal data, emphasizing the need for practical solutions derived from empirical observations to bridge this gap and enhance user data protection in digital interactions.

Leveraging Large Language Models (LLMs) like BARD, OCRA and GPT, this work aims to automate the summarization of privacy policies [4]. Specifically focusing on GDPR compliance, the proposed system extracts and highlights clauses related to PII sharing, identifies and categorizes sensitive and non-sensitive data, and specifies the location and context of data usage. The goal is to provide users with concise summaries, ensuring transparency and aiding in assessing compliance with privacy regulations.

Key contributions of this paper include:

- Privacy Policy Retrieval: Users can input a URL to retrieve the privacy policy of a specific website.

*Place the footnote text for the author (if applicable) here.

IC3 2024, August 08–10, 2024, Noida, India

ACM ISBN 979-8-4007-0972-2/24/08
https://doi.org/10.1145/3675888.3676142

Table 1: Styles available in the Word template

Parameter	[9]	[10]	[11]	[12]	[13]	[14]
Purpose	Using AI to support compliance with GDPR	Using Models to Enable Compliance for GDPR	Deep Learning based Policies' Compliance of GDPR	Prompt Pattern Catalog for ChatGPT	NLP-Based Automated Compliance of GDPR	Using LLMs for GDPR Compliance in Cookie Banners
Approach Used	Reviewed requirements of compliance documents	UML and OCL representation of GDPR	CNN-based model with active learning	Enrich conversational LLM prompts	Semantic frame representations- Similarity metrics	Large language models (GPT-3) Static code analysis- Web scraping
Algorithms Used	Proposed Using any rule-based AI	Generate Domain specific instance model from generic UML	CNN-based multi-class classifier predict presence of sensitive data	CNN based text classification model	Cosine similarity- Wu-Palmer similarity- Jaro Winkler distance	Contextual HTML and Browser attributes

- Language Model Integration: The system employs Large Language Models (LLMs) from Google Bard and OpenAI GPT 3.5 to analyze privacy policies.
- GDPR Compliance Evaluation: The tool evaluates whether the fetched privacy policies comply with GDPR regulations.
- Data Categorization: The system categorizes and describes sensitive and non-sensitive data found in privacy policies.
- User-Friendly Frontend: The work incorporates a Streamlit frontend, ensuring a simple and intuitive interface for users.

Rest of the paper is organized in four sections. Section 2 discusses the related work done in privacy policy interpretations. Section 3 describes the methodology of prompt engineering for the underlying problem. Section 4 presents the results of GDPR compliance of some real-world privacy policies. Section 5 concludes the work by outlining the future directions of work in this area.

2 RELATED WORK

This work's proactive stance in warning users and restoring confidence in digital interactions is grounded in the empirical reality of privacy issues observed in real-world cases. A bitter example of such misuse occurred in the infamous case involving Cambridge Analytica and Facebook in 2018 [5]. In this real-life scenario, Cambridge Analytica, a political consulting firm, accessed and utilized the personal data of millions of Facebook users without their explicit consent. In this section, existing tools and techniques for easy interpretation of complex privacy policies are reviewed.

2.1 Existing Tools

Several tools have emerged to tackle the challenges of privacy compliance and effective cookie management. Notable among these are OneTrust[6], Cookiebot[7], and Privacy Badger[8]. OneTrust [6], a comprehensive privacy management platform, equips organizations with a suite of tools to navigate and comply with privacy regulations such as GDPR. Its features encompass cookie consent management, data mapping, risk assessment, and incident response. With a specific focus on GDPR compliance, OneTrust facilitates tasks like managing Data Subject Requests (DSRs) and conducting Data Protection Impact Assessments (DPIAs).

Cookiebot [7], on the other hand, specializes in cookie consent management. It automatically scans websites to categorize and manage cookies, presenting a customizable consent banner to visitors. It goes a step further by enabling automatic cookie blocking for users who decline specific cookies and offers additional tools for GDPR compliance, including data processing records and consent documentation.

Privacy Badger [8], a user-friendly browser extension, addresses privacy concerns by blocking trackers and cookies that infringe upon user privacy, all without the need for user configuration. It operates as a privacy-enhancing tool, providing users with increased control over their online tracking preferences.

These solutions exemplify the diverse approaches available to organizations and individuals seeking to manage cookies and address privacy concerns, from comprehensive privacy management platforms to specialized consent management tools and user-centric browser extensions.

2.2 Existing Research

Authors in [9] enlist the important cases of GDPR compliance where AI/ML based techniques may be useful. These included adhering to compliance checklists, facilitating risk assessments of data exposure, meeting requirements of new regulations and thwart automatic profiling by imposters. AI based methods have been shown to support in all facets of privacy preservation of user data.

Use of cookies on websites and their implications for privacy and cybersecurity is discussed in [10]. It provides an overview of different cookie types, including session cookies, persistent cookies, and third party tracking cookies. The author reviews how cookies can monitor user online activities and thereby pose threats to privacy. However, the paper also notes that cookies themselves do not directly access private user information on devices - they

only store data that users submit to websites. The discussion then covers potential cybersecurity issues stemming from cookies. This includes vulnerabilities in access control schemes if session cookies are compromised. The paper also examines how malicious websites could leverage cookies to gather and misuse private user data. Finally, the author recommends methods for enhancing privacy and security regarding cookies, like deleting cookies regularly and using anonymizing tools. Overall, while recognizing that cookies raise legitimate privacy concerns, the paper concludes that cookies are not inherently malicious but rather depend on how online entities design and manage them.

[11] presents a study analyzing the compliance of privacy policies with the EU's General Data Protection Regulation (GDPR). The authors create a dataset of 1080 privacy policies manually annotated by experts with 18 categories representing GDPR disclosure requirements. They then develop a Convolutional Neural Network (CNN) model to classify privacy policy segments into these 18 GDPR classes with 89.2% accuracy. Through active learning, the model reaches this level of performance with very less additional training data. The authors apply the model to privacy policies of about 10000 websites. They made an interested finding that about 68% of them did not fully comply with GDPR - failing on at least one requirement. Surprisingly, critical requirements like disclosing profiling details or data storage periods are only covered by 28-45% of websites. The paper also conducts a user study where around 32% of people struggled understanding policies explaining GDPR rights. Overall, the work contributes both a useful privacy policy dataset and an accurate classification model to automate GDPR compliance checking at scale. The findings reveal most websites need improvement to align their policies with GDPR law.

[12] introduces the concept of "prompt patterns" as a structured way to document effective prompts that solve common problems when interacting with large language models like ChatGPT. Prompt patterns are analogous to software design patterns. It provides a framework for documenting prompt patterns including intent, motivation, structure, example implementation, and consequences. The paper presents a comprehensive catalog of 16 initial prompt patterns. These prompts were categorized on the basis of semantics, error detection and customization. They also show how the patterns can be combined and composed to create more complex capabilities. Discusses lessons learned regarding the utility of prompt patterns and need for further research into developing a more complete prompt pattern language.

[13] This paper provides an examination of LangChain, an open-source software library for rapidly developing custom AI applications using large language models. It focuses on LangChain's core components like prompts, chains, memory, and agents and demonstrates use cases like question answering over documents. The study aims to spur further exploration of tools like LangChain for streamlining large language model application development.

[14] This paper presents a tool for automatically analyzing the GDPR compliance of cookie banners on websites. It uses a combination of large language models and static code analysis to locate cookie banners and check attributes like consent mechanisms, information provided, and accessibility. An evaluation by a legal expert found the tool approaches human capabilities in identifying violations. The research contributes both a practical instantiation and a novel technical method for automated legal compliance analysis.

[15] This paper investigates using natural language processing techniques to automatically compare privacy laws similar to GDPR across different countries. It transforms legal documents into structured data and applies methods like TF-IDF, word embeddings, BERT embeddings, and siamese networks to measure document similarity. A preliminary experiment between GDPR and Brazil's LGPD found BERT achieved the best performance. The research contributes a structured GDPR-like document dataset and baseline results to enable future research on automatic legal document analysis.

[16] This paper discusses the phenomenon of emergent abilities in large language models, which refer to abilities that are not present in smaller models but emerge in larger models. It provides a formal definition of emergence and surveys examples of emergent abilities in areas like few-shot prompting, reasoning, and model calibration. The paper also discusses potential explanations and future directions for research on emergence.

3 METHODOLOGY OF PRIVACY POLICY INTERPRETATION

3.1 System Model

Our proposed solution involves the development of an innovative system utilizing Large Language Model (LLM) technology. This system aims to automate the summarization of lengthy and complex privacy policies prevalent across various websites and online platforms. By employing advanced natural language processing techniques, the system will extract and highlight critical information within these policies, focusing particularly on personally identifiable information (PII) sharing and compliance with global privacy laws. Figure 1 shows the system model and use case diagram with system and end users. End users can enquire about the policy compliance by giving URL of the policy and model of his choice. The system side code runs the logic for compliance checking and returns the exact data being shared under the policy. Main goal of the proposed approach is to enhance user comprehension by summarizing complex privacy policies, thereby empowering users to make informed decisions regarding their online privacy.

3.2 GDPR Overview

GDPR is a regulation passed by European Union (EU) in 2016 and applies to all its members [17]. Organizations worldwide have adopted it for regulating privacy breach of individuals. It ensures requirement of affirmative consent from individuals for data processing. It also grants individuals rights to access, rectify, erase, and port their data. GDPR obligates organizations to report data breaches within 72 hours as well as integrate data protection into processing activities and systems. The implementation is ensured by levying heavy fine in case of non-compliance. National Data Protection Authorities (DPAs) have been setup to overlook the enforcement of the regulation in spirit.

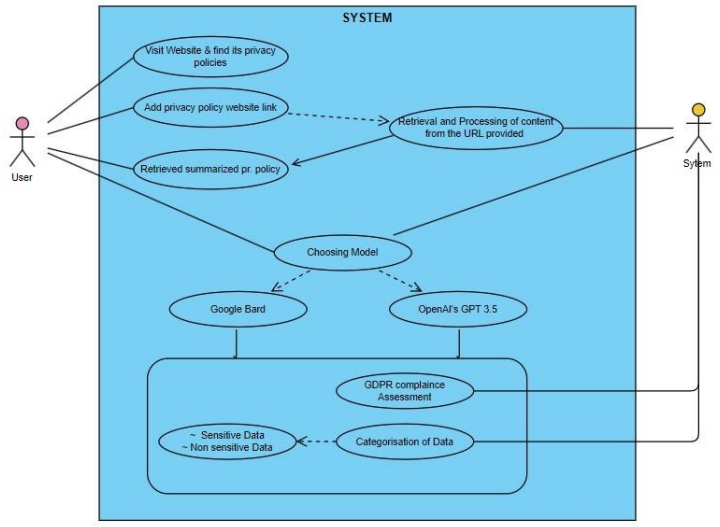

Figure 1: System Model

```
demo_template = '''
Summarize the privacy policy of this
{text}
 with a focus on how it handles user PII, in compliance with GDPR and Indian privacy laws

'''
```

```
'BMW Group India recognizes the importance of protecting PII of its users, including Sensitive Personal Information, provided
by natural persons, under lawful contract. BMW Group India intends to take reasonable measures to keep such information
confidential and may share it with its affiliates and third parties under appropriate arrangements and under the applicable
laws and policies. Personal Information/Sensitive Personal Data is collected and used/processed for lawful, legitimate,
contractual and administrative purposes of BMW Group India. BMW Group India would not disclose any Personal
Information/Sensitive Personal Data to any external organization unless it has the consent of the provider, or are required by
law or have previously informed the Provider. BMW Group India has in place a security system, to ensure that the personal
information is protected from unauthorised access, use, disclosure or alteration by anyone including the employees of BMW
Group India. BMW Group India may render the Personal Information/Sensitive Personal Data anonymous or pseudonymised, once the
purpose of the processing of Personal Data is fulfilled. BMW Group India also allows users to review and change their personal
information on request and provides a contact (Grievance Officer) for any discrepancies or grievances related to the
processing of information.'
```

Figure 2: Zero-Shot Prompting for a Sample Privacy Policy Interpretation

3.3 Prompt Engineering

Prompt engineering is a technique used to design and refine input prompts (instructions) for LLMs to elicit desired responses. In case of privacy policy interpretation, it is important to get precise and reliable information and thus prompt engineering techniques were applied to test the appropriateness of output. Zero-shot and chain of thought prompting methods have been defined to summarize key aspects of GDPR/privacy law compliance from policy text. In Zero-shot prompting, the model is given a task without any prior examples, relying solely on its pre-trained knowledge. In this case , it is considered that GDPR is world-wide regulation and LLM must have been trained on its content, a zer-shot prompt of directly summarizing the policy document was tried.

Figure 2 shows the prompt designed on this method and output interpretation of policy. The broad context of task is given with respect to GDPR, PII and Indian privacy laws.

In contextual prompting, additional context or background information is provided to shape the response. Figure 3 shows the contextual prompt designed to obtain the exposure of sensitive data and its usage. In order to get the appropriate information that we are seeking, the prompt of Figure 3 was presented to LLMs in few variations. Output of interpretations for three of them are given in Figure 4, Figure 5 and Figure 6.

Prompt shown in Figure 4 is designed to ensure whether the organization provides clear and accessible information about data processing as per Article 12 of GDPR. Another variation in Figure 5, is about compliance to article 13 and 14 of GDPR that states about the data subjects having the right to be informed about the

GDPR Compliance: Evaluate if the policy complies with GDPR.
PII Handling: Categorize and describe sensitive and non-sensitive data in the policy, and briefly mention where and how each is used.
Sensitive Data:
List types of sensitive data.
Describe where and how each is used briefly.
Non-Sensitive Data:
List types of non-sensitive data.
Describe where and how each is used concisely.

Figure 3: Design of Contextual Prompt for Generic Privacy Policy Interpretation

```
Summarize the following extracted text related to personally identifiable information (PII) sharing and privacy laws: {text}
Ensure that the summary aligns with GDPR principles, including:
- Data minimization: Explain how the collected data is minimized to what is necessary for the specified purpose.
- Consent: Describe how individuals' consent is obtained and the right to withdraw it.
- Data protection rights: Highlight individuals' rights to access, rectify, and erase their data.
- Data security: Discuss the measures in place to secure PII and prevent data breaches.
- Cross-border data transfers: Explain how international data transfers are handled in accordance with GDPR.
'''
'\nThe BMW Group India is committed to data privacy and protection, ensuring the safety of Personal Information and Sensitive Personal Data (SPD) of its customers, employees, suppliers, and shareholders. Personal Information and SPD is collected and used for lawful purposes such as administrative and contractual operations, marketing surveys, customer research, warranty services, and to fulfill legal and regulatory obligations. It is only shared within the affiliates and/or group companies, authorized BMW and MINI dealers, and other authorized business partners. BMW Group India has implemented security measures to ensure that personal information is protected from unauthorized access, use, disclosure, or alteration, and follows the international standard ISO 27001 for its Information Security Management System. Data minimization is also practiced, with access to personal data granted only to personnel on a need-to-know basis. Consent is obtained from individuals before their data is used, and they can opt-out at any time. Individuals also have the right to access, rectify, and erase their data. International data transfers are handled in accordance with GDPR.'
```

Figure 4: Contextual Prompting for a Sample Privacy Policy Interpretation – Prompt 1

```
demo_template = '''
Summarize the privacy policy of this
{text}
 with a focus on how it handles user PII, in compliance with GDPR and Indian privacy laws.

*GDPR Compliance:*
Assess whether the privacy policy complies with GDPR standards. Indicate any areas of non-compliance if
present, in plain language.

*Use of Personally Identifiable User Information:*
Categorize and describe what user information is collected, distinguishing between critical (sensitive) and
non-critical (non-sensitive) data. Explain where and how each type of data is used, as mentioned in the
privacy policy.

Evaluate the clarity and simplicity of the policy in conveying these data practices for the benefit of
non-technical individuals.
give the answer in bullet points
'''
```

```
- The privacy policy complies with GDPR standards.
- User information collected includes both critical (sensitive) data such as password, financial information and health-related data, as well as non-critical (non-sensitive) data such as name, address and contact information.
- Sensitive data collected is used for administration and facilitation of relationship with customers, employees, suppliers etc., for marketing surveys and customer research and feedback, and for satisfying legal and regulatory obligations.
- Non-sensitive data is used for internal operational purposes, to update users with information about BMW Group India and its products and services, and to provide information about special offers.
- The privacy policy is clear and simple in conveying data practices, making it accessible to non-technical individuals.
```

Figure 5: Contextual Prompting for a Sample Privacy Policy Interpretation – Prompt 2

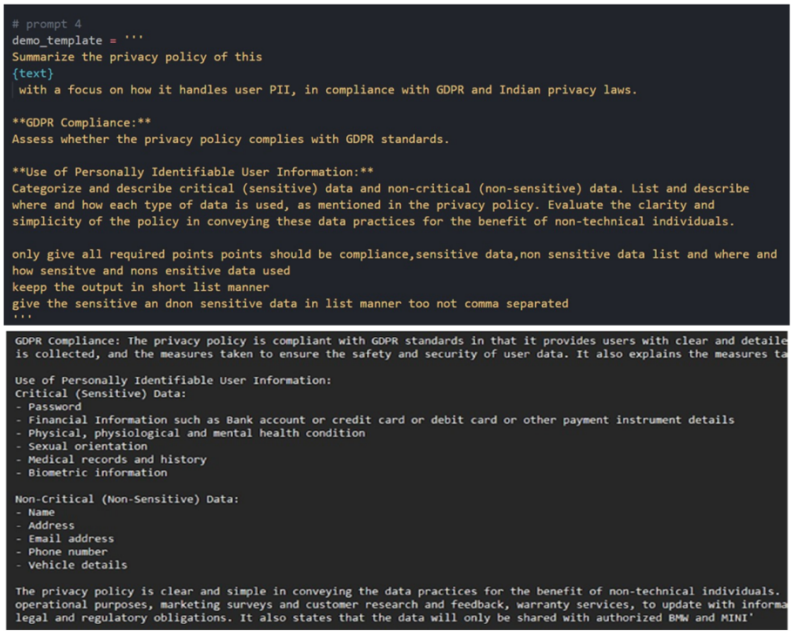

Figure 6: Contextual Prompting for a Sample Privacy Policy Interpretation – Prompt 3

collection and use of their data. Figure 6 defines a variation of seeking data sharing information with details on how to present the information systematically. The readable output from these prompts will be useful for user to take decision about their data processing, portability and automated profiling by third-parties.

It can be seen that the contextual prompting has enhanced the interpretation of privacy policy and improved user understanding. Users receive simplified explanations addressing their specific concerns, facilitating informed consent and risk assessment. Variations of contextual prompts show that accurate interpretations are consistent and will aid in decision making about the privacy footprint of the website.

3.4 Automated Privacy Policy Retrieval and Interpretation

First step involves fetching privacy policies from URLs using the polipy library, which includes the following steps:

- URL Input: Users provide URLs through the interface to retrieve the privacy policies associated with those links
- Fetching Policies: The system sends requests to the provided URLs and retrieves the privacy policy documents.
- Processing Policies: Upon retrieval, the policies are further processed to extract the text content and standardize the format for analysis. It includes removing unnecessary information like header, footer, or navigation information that is not part of the privacy policy text itself.

Two options have been worked out for LLM Model Integration namely:

- Google Bard via Langchain: The Google Bard model integration is accomplished through the Langchain library, which facilitates communication with the Google Bard API. The model specializes in assessing GDPR compliance with privacy policies. It categorizes data into sensitive and non-sensitive types, evaluating compliance against predefined templates or instructions. It uses specific prompts or templates to guide the model in extracting insights, such as GDPR compliance evaluation and categorization of data. fetch_Bard_Insights(privacy_policy) that uses a natural language processing model to summarize the privacy policy regarding its compliance with GDPR and Indian privacy laws. An API key (api_key) is defined to get access to the Google Bard.
- OpenAI GPT-3.5 via Langchain: The integration with OpenAI's GPT-3.5 model is also through Langchain, enabling interaction with OpenAI's API. The GPT-3.5 model from OpenAI excels in summarizing privacy policies, assessing GDPR compliance, and categorizing data types based on provided prompts or instructions. It is similar to Google Bard, it relies on specific prompts or templates to guide the model in generating insights, evaluating GDPR compliance, and categorizing data within privacy policies.

3.5 LLMChain Setup

An instance of the GooglePalm class is created, possibly representing a natural language processing model using the Google PALM (Pattern Learning Model) API. The API key is passed as a parameter, and the temperature parameter is set to 0.7, controlling the randomness of the model's output. An instance of the LLMChain class is created, combining the language model (llm) and the prompt template (prompt). The chain.run(privacy_policy) method is called to process the privacy_policy text using the defined template and

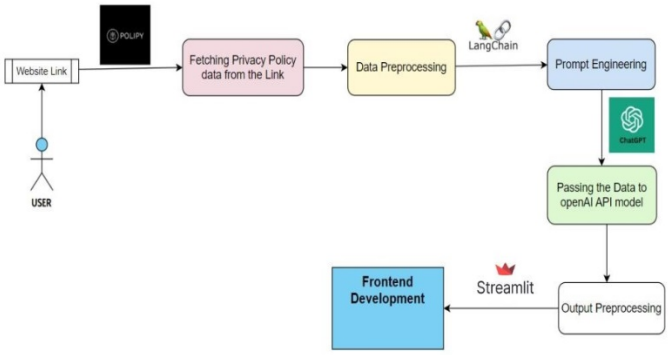

Figure 7: Data Flow Model

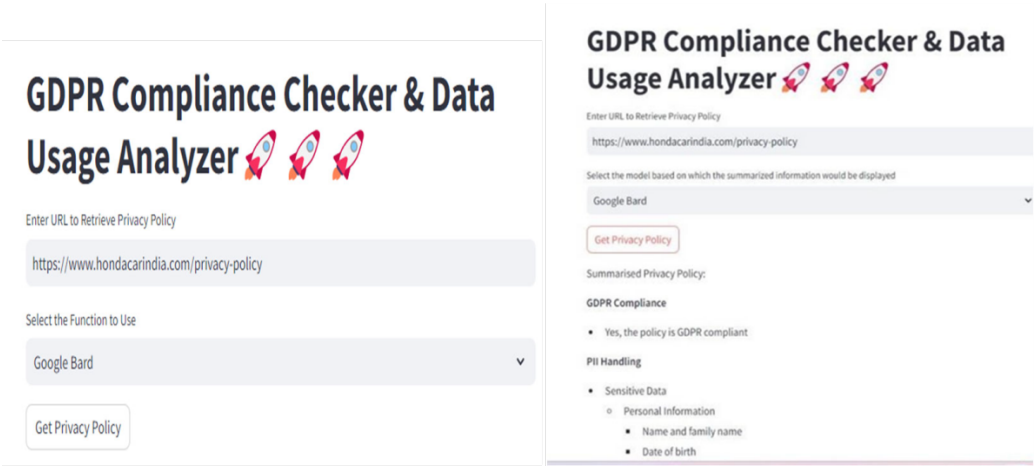

Figure 8: Privacy Policy Interpretation of Honda Cars – Successful Compliance

language model. The result is stored in the text variable. The function returns the text variable, which presumably contains the summarized insights extracted from the privacy policy. The Streamlit frontend takes the URL input and policy text. It allows selecting either Google Bard or OpenAI to process the text. It displays the generated compliance summary response. The complete flow model is shown in Figure 7.

4 IMPLEMENTATION AND TEST RESULTS

4.1 Examples of Real-World Policies

Privacy policies of quite a few websites were analyzed using the proposed method.

Figure 8 show the privacy compliance checking of Honda cars privacy policy in India. The output shows that their policy complies to GDPR requirements of data sharing and doesn't transmit the user data anywhere. On the other hand as shown in Figure 9, another popular website of an ornaments company (name has been omitted) fails to comply the privacy requirements.

4.2 Limitations

The proposed work is effective in privacy policy interpretations, but still lacks on some points. The use of OpenAI comes with a token limitation, which may impact the processing of lengthy privacy policies. Large documents might need to be truncated or processed in segments, potentially affecting the accuracy of the summarization. Privacy policies across different websites may vary significantly in structure and content. Handling diverse formats and language styles could pose a challenge, leading to variations in the effectiveness of the summarization process. While efforts are made to evaluate GDPR compliance, the automated system may not capture nuanced legal language, and its assessment might not substitute for a thorough legal review. The system's accuracy in identifying compliance may be subject to the complexity and specificity of legal terminology.

5 CONCLUSIONS

The work lays the foundation for future enhancements and optimizations. To refine the system, there's a focus on improving the algorithms driving machine learning models, aiming for increased

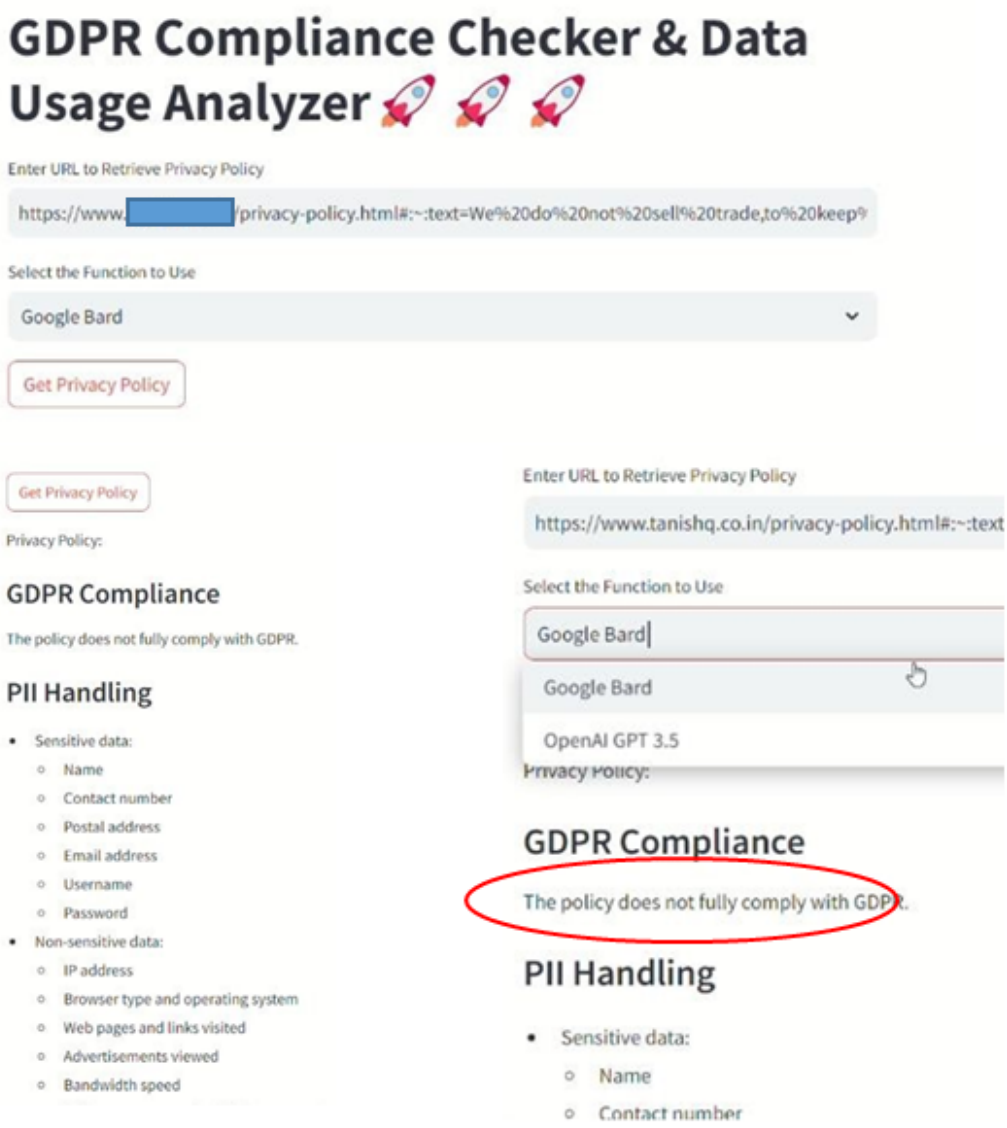

Figure 9: Privacy Policy Interpretation of Tanishq – Unsuccessful Compliance

precision and accuracy. The ongoing effort includes optimizing time complexities, reducing processing power requirements, and ensuring sustainable infrastructure. Future iterations of the work will expand the scope by incorporating additional language models and datasets. This expansion will allow the system to address a broader range of privacy concerns and contribute to a more comprehensive understanding of various privacy policies. The user experience can be a key area of focus for future development. The system can be made more user-centric and aligned with the evolving needs of digital privacy governance.

REFERENCES

[1] Jozani, Mohsen, Emmanuel Ayaburi, Myung Ko, and Kim-Kwang Raymond Choo. "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective." Computers in Human Behavior 107 (2020): 106260.
[2] Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age." Journal of Consumer Psychology 30, no. 4 (2020): 736-758.
[3] Karegar, Farzaneh, John Sören Pettersson, and Simone Fischer-Hübner. "The dilemma of user engagement in privacy notices: Effects of interaction modes and habituation on user attention." ACM Transactions on Privacy and Security (TOPS) 23, no. 1 (2020): 1-38.
[4] Nadikattu, Ashok Kumar Reddy. "COOKIES PRIVACY AND CYBER SECURITY." International Journal of Creative Research Thoughts (IJCRT), ISSN: 2320-2882.
[5] Isaak, Jim, and Mina J. Hanna. "User data privacy: Facebook, Cambridge Analytica, and privacy protection." Computer 51.8 (2018): 56-59.
[6] https://www.onetrust.com/ [Accessed on 14 May 2024]
[7] https://www.cookiebot.com/ [Accessed on 14 May 2024]
[8] https://privacybadger.org/ [Accessed on 14 May 2024]
[9] Kingston, John. "Using artificial intelligence to support compliance with the general data protection regulation." Artificial Intelligence and Law 25.4 (2017):

429-443.
[10] Torre, Damiano, *et al.* "Using models to enable compliance checking against the GDPR: an experience report." 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS). IEEE, 2019.
[11] Rahat, Tamjid Al, Minjun Long, and Yuan Tian. "Is Your Policy Compliant? A Deep Learningbased Empirical Study of Privacy Policies' Compliance with GDPR." Proceedings of the 21st Workshop on Privacy in the Electronic Society. 2022.
[12] White, Jules, Quchen Fu, Sam Hays, Michael Sandborn, Carlos Olea, Henry Gilbert, Ashraf Elnashar, Jesse Spencer-Smith, and Douglas C. Schmidt. "A prompt pattern catalog to enhance prompt engineering with chatgpt." arXiv preprint arXiv:2302.11382 (2023).
[13] Amaral, Orlando, Muhammad Ilyas Azeem, Sallam Abualhaija, and Lionel C. Briand. "Nlp-based automated compliance checking of data processing agreements against GDPR." IEEE Transactions on Software Engineering (2023).
[14] Otterström, Marcus, and Oliver Palonkorpi. "Cookie Monsters: Using Large Language Models to Measure GDPR Compliance in Cookie Banners Automatically." (2023).
[15] Kawintiranon, Kornraphop, and Yaguang Liu. "Towards automatic comparison of data privacy documents: a preliminary experiment on gdpr-like laws." arXiv preprint arXiv:2105.10117 (2021).
[16] Topsakal, Oguzhan, and Tahir Cetin Akinci. "Creating large language model applications utilizing langchain: A primer on developing llm apps fast." In International Conference on Applied Engineering and Natural Sciences, vol. 1, no. 1, pp. 1050-1056. 2023.
[17] Mondschein, Christopher F., and Cosimo Monda. "The EU's General Data Protection Regulation (GDPR) in a research context." Fundamentals of clinical data science (2019): 55-71.