iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80854

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Hybrid Explainable AI and Knowledge Graph Framework for Dynamic Multi-Jurisdictional Privacy Law Compliance

Kalyani K. Thakare
Research Scholar, Department of Computer Engineering, Thakur College of Engineering & Technology, Mumbai, India

Abstract: ***Global data privacy laws, such the EU's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and India's Digital Personal Data Protection (DPDP) Act, are constantly changing and vary by jurisdiction, making compliance extremely difficult. Current AI-based compliance technologies are frequently opaque, poorly linked with functional IT systems, and sluggish to adjust to changes in the law. In order to facilitate auditable, low-latency compliance management, this article suggests a hybrid Regulatory AI (RegAI) system that integrates natural language processing, explainable AI(XAI), and a privacy-ontology-driven knowledge graph. The system uses two input modes: (i) text-text comparison and (ii) text-URL comparison of official legal documents. It also performs clause-level mapping, ingests regulatory texts and updates, and compares old and new versions of legislation. For GDPR, CCPA, and DPDP Act compliance reasoning, the knowledge graph is the only source of truth. Accuracy, transparency, and latency are evaluated experimentally using realistic regulation change scenarios. The possibility of dynamic, explainable compliance automation is demonstrated by the results, which show high clause-mapping accuracy, comprehensible explanations for compliance judgments, and near-real-time processing of legal modifications.***

Keywords: Natural Language Processing (NLP), Explainable Artificial Intelligence (XAI), Regulatory AI (RegAI), Knowledge Graphs, Privacy Ontology.

I. INTRODUCTION

Globally, data privacy is becoming a major regulatory problem. Organizations are subject to specific requirements concerning data collecting, processing, sharing, and user rights under the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Digital Personal Data Protection (DPDP) Act. Significant penalties, harm to one's reputation, and a decline in confidence can result from noncompliance. The legal environment is continuously evolving as regulations are modified, clarified, and interpreted through guidelines and enforcement rulings.

Businesses are looking more and more for AI-based support to monitor and carry out regulatory requirements. However, there are three typical issues with present systems:

A. Black-box decision-making:

Machine-learning algorithms don't explain why certain behaviors are marked as compliant or non-compliant [3], [9].

B. Inadequate flexibility:

Models frequently need retraining or significant reconfiguration when requirements change [6].

C. Limited IT system integration:

Data flows, APIs, and contracts are examples of operational artifacts that are difficult to link to compliance logic [4].

In order to overcome these issues, this work develops and assesses a hybrid Regulatory AI (RegAI) architecture that:

1) Creates a formal, auditable knowledge graph by encoding legal requirements from the DPDP Act, CCPA, and GDPR.
2) Performs clause mapping and old-new law comparison using Natural Language Processing (NLP) techniques.
3) Explains forecasts and suggestions at the clause and document levels using SHAP.
4) Provides performance measures for latency, accuracy, and transparency that may be included into workflows for continual compliance.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

II. BACKGROUND AND RELATED THEORY

A. International Data Privacy Laws

GDPR: Provides extensive guidelines for handling people's personal data within the EU, with a focus on data subject rights, fairness, lawfulness, and openness.
CCPA: With ideas like "opt-out of sale," the CCPA focuses on consumer rights in California with regard to data sale, sharing, and disclosure.
DPDP Act: The DPDP Act, which introduces data protection rights and obligations in the Indian context, is similar to some GDPR concepts but has different enforcement mechanisms and a different scope.
In terms of definitions, responsibilities, and remedies, these regulations overlap but also differ [11]. Both shared and unique provisions must be understood by multijurisdictional enterprises.

B. The Environment of Compliance Automation

Existing work has developed:
Cloud and Big Data compliance using GDPR and Payment Card Industry Data Security Standard (PCI DSS) KGs [1].
Knowledge Graphs (KG)-based methods for contract-based GDPR verification and informed consent [5].
NLP-based completeness and violation detection for DPAs and privacy policies [3], [12].
Policy-regulation alignment using LLM+KG frameworks [19].
Nevertheless, they rarely provide post-hoc XAI over hybrid pipelines and unified multi-law change tracking with explicit change-ratio metrics.

C. Ontologies and Knowledge Graphs

Legal concepts, obligations, roles, dangers, and controls are represented in machine-readable ways by knowledge graphs and ontologies [8]. They facilitate traceability from abstract concepts to specific technological measurements, logical reasoning, and consistency testing. Previous GDPR and PCI DSS ontologies show how security controls can be related to articles, roles (controller, processor), and obligations [4],[10].

D. Natural Language Processing (NLP) for Legal Text

Automated requirements extraction, semantic similarity analysis, and classification of legal provisions and privacy paperwork are made possible by NLP[3]. Among the methods are:
Sentence and phrase embedding, as well as BERT-based similarity for clause alignment [11],[14].
Text classification to identify if requirements are met or not[15].
Natural Language Inference (NLI)-style comparison of policies and regulations [16].

E. Explainable AI

Explainable AI uses post-hoc techniques like SHAP to make model outputs comprehensible to humans. AI-based policy and DPA analyzers emphasize the requirement for transparency, accountability, and auditable decision routes [9],[15], whereas the majority of privacy compliance work concentrates on semantic transparency through KGs and rule models .

III. LITERATURE SURVEY

Prior research highlights:

A. *Knowledge Graphs in Compliance*: GDPR and PCI DSS ontologies connecting obligations to Cloud Security Alliance (CSA) controls [10]. GDPR cloud data control ontologies modeling roles and obligations [4]. KG-based tools for GDPR consent and contracts, enabling automated verification [5],[8]. Integrated KGs for cloud data regulations capturing threats, controls, and overlapping rules [1].
B. *Policy and Data Processing Agreement (DPA) Analysis Using NLP and ML*: GDPR and cloud privacy policies kept in a KG [14] are semantically identical. AI-enabled completeness checking of DPAs and privacy policies utilizing highly accurate supervised learning and language models with F-scores of [12], [15]. NLI-based GDPR policy violation detection [16]. Scalable privacy policy annotation using large language models [9].

©IJRASET: All Rights are Reserved

C. *Large Language Model (LLM) + KG Hybrid Approaches:* PrivComp-KG uses Retrieval-Augmented Generation [2], [18] to relate vendor policies to GDPR/CCPA-like regulations. LLM+KG framework for high semantic accuracy in IoT GDPR compliance Q&A [19].

D. *Analysis of Multiple Jurisdictions:* GDPR and CCPA [11] convergence and divergence are analyzed using Bidirectional Encoder Representations from Transformers (BERT) and clustering. An examination of privacy practices spanning several years, including the impact of GDPR/CCPA [13], [17]. The suggested RegAI framework is informed by these works, but they do not provide dynamic, explainable, multi-law change-ratio computation rooted in an auditable KG.

IV. MOTIVATION AND OBJECTIVE

Four ongoing gaps are the driving force behind this project:

1) Dynamic change management: While guidelines and regulations change, most tools assume the legislation as static, necessitating extensive manual updates or retraining [14].

2) Explainability at the legal-clause level: Organizations must comprehend which clauses raised a compliance flag and how to address it [3].

3) Multi-law, clause-level comparison: Businesses that operate internationally must maintain consistent internal policies and compare their responsibilities under the DPDP Act, CCPA, and GDPR [11],[17].

4) Auditability and integration: IT systems need machine-readable rules [8]; regulators and auditors demand repeatable, evidence-based reasoning chains.

By integrating an auditable KG, NLP clause mapping, change-ratio measurements, and XAI, the suggested RegAI framework satisfies these requirements.

Following are the objectives of the project:

a) For at least the GDPR, CCPA, and DPDP Act, create a privacy ontology and knowledge graph that captures legal frameworks, rights, obligations, roles, and enforcement ideas.

b) Calculate change ratios between versions at the article and clause levels by applying clause mapping and old-new law comparison using NLP.

c) Dual input options are supported: (i) old/new law texts; (ii) old law text and new law URL, with automated parsing and retrieval.

d) Integrate explainable AI (SHAP) to offer human-readable justifications for change detection and compliance categorization.

e) Analyze performance in three areas: latency, accuracy, and transparency.

V. STATEMENT OF CONTRIBUTION

The following are the contributions of this work:

A formal privacy ontology and KG that serves as the single source of truth for compliance logic and unifies key ideas from the CCPA, DPDP Act, and GDPR.

A pipeline for mapping clauses that generates structured alignments and similarity scores between (a) various laws and (b) variations of the same legislation.

A change-ratio metric that measures how much the law has changed at various levels of detail (clause, article, thematic area).

A hybrid RegAI architecture that combines SHAP explanations, KG reasoning, and NLP models into a logical compliance workflow.

A dataset design and empirical evaluation approach for assessing latency, correctness, and transparency in practical regulatory updating scenarios.

The primary innovative contributions are:

Instead of employing any one method in isolation, a hybrid RegAI architecture for regulatory change management closely integrates a legal knowledge graph, NLP-based clause mapping, and post-hoc XAI (SHAP) [3].

Using two input modes (text–text and text–URL), multi-jurisdictional change-ratio computation is used to compare old and new versions of GDPR-, CCPA-, and DPDP-like regulations at the clause level.

Knowledge base for auditable compliance in which the KG is the sole source of truth and every choice can be linked to certain articles, clauses, and ontology entities [1],[5].

Low latency and constant updates are the goals of an operationally integrated architecture that addresses the scalability and adaptability issues with compliance tools [1].

VI. METHODOLOGY

A. *Knowledge Graph Design and Ontology*

1) Identification of Concepts: From the GDPR, CCPA, DPDP Act and earlier ontologies [4],[5], extract key legal entities (data subject, controller, processor, permission, legal basis, right to erasure, sale of personal data, etc.).

2) Definition of a Schema: To model roles, responsibilities, rights, prohibitions, remedies, and enforcement actions, define classes, properties, and constraints. To keep track of several legal versions and jurisdictions, incorporate versioning metadata.

3) KG Execution: Use ontology in RDF/OWL or a similar graph data paradigm.

Use an initial semi-automated pipeline [1] to populate with clause-level instances from regulatory texts.

B. *Mapping Clauses and Calculating Change Ratios*

1) Embedding and Pre-processing

Divide regulations into clauses with numbers.

Use a domain-tuned transformer model (such as legal-domain BERT) to create embedding.

2) Alignment and Similarity

Calculate the cosine similarity between each source clause and candidate target clauses [11], [14].

Choose the top k matches that are over a certain threshold as alignments, then store the alignment kinds and scores in the KG.

3) Metric of Change-Ratio

Describe the categories of changes (e.g., added, removed, modified, rephrased, enlarged, narrowed).

Features from ontology annotations, length differences, and similarity scores are used to train a classifier.

Determine the change ratio for each article and law.

C. *Integration of Explainable AI*

1) Model Choice

For impact prediction and clause change classification, employ supervised models (such as shallow neural nets and gradient boosting).

2) Application of SHAP

To determine feature importance per prediction, use SHAP (e.g., similarity scores, term-level differences, ontology class features).

3) Storage Explanation

Explanation artifacts should be serialized and linked to the appropriate clause mapping and decision nodes in the KG.

A. *Evaluation*

1) Datasets

Create an ideal collection of clause mappings and switch labels between:

Two subsequent iterations of legislative documents similar to GDPR (e.g., regulation vs. consolidated version).

Selected overlapping clauses of the CCPA and GDPR-CCPA [11]. Draft and adopted texts of the DPDP Act.

2) Baselines

Simple classifiers without KG features or XAI [14]. Keyword-based and unsupervised similarity techniques.

3) Metrics

Clause mapping and change categorization accuracy and F1 (in line with previous studies [3]).

Expert assessments of explanation usefulness [9],[15] and explanation coverage demonstrate transparency.

End-to-end processing time for each legal update and clause; scalability for document sizes [1], [5].

B. *RegAI Framework*

The following modules make up the RegAI framework and are connected by the KG:

Module 1: Regulation Ingestion

- Either consumes raw text documents or retrieves legal texts from official sources (URLs).
- Divides documents into articles, sections, and clauses, which are structural units.

Module 2: NLP Processing and Clause Mapping

- Carries out sentence embedding (e.g., transformer-based), tokenization, and POS-tagging.
- Determines the semantic similarity between clauses from various versions or laws.
- Generates mapping candidates with scores on similarity.

Module 3: Layer of Knowledge Graph

- Keeps instances of legal ideas, clauses, rights, duties, and relationships in ontology.
- Documents change-ratio annotations, similarity scores, and clause mappings.

Module 4: Layer of Explainable AI

- SHAP is used by classifiers (such as those for "changed," "unchanged," and "broadened obligation") to explain feature contributions.
- Clauses and decisions have explanation objects attached as KG metadata.

Module 5: Decision-Making Engine for Compliance

- Creates alerts and suggested adjustments by using KG reasoning and ML outputs to assess the influence on organizational policies and controls.

Module 6: Integration and Interfaces

- Dashboards and APIs for IT, legal, and compliance users.
- Hooks for integrating with Continuous Integration and Continuous Deployment (CI/CD) pipelines, ticketing systems, and policy repositories.

C. Two Input Modes

Mode 1: Comparison of Texts

- Text copies of both the old and new laws are available.
- The system calculates change-ratios, updates KG, and maps direct clauses.

Mode 2: Comparing Text and URLs

- The new law is indicated by the official document URL, while the old law is given as text.
- Before executing the same mapping pipeline, the ingestion module retrieves, cleans, and segments the new law.

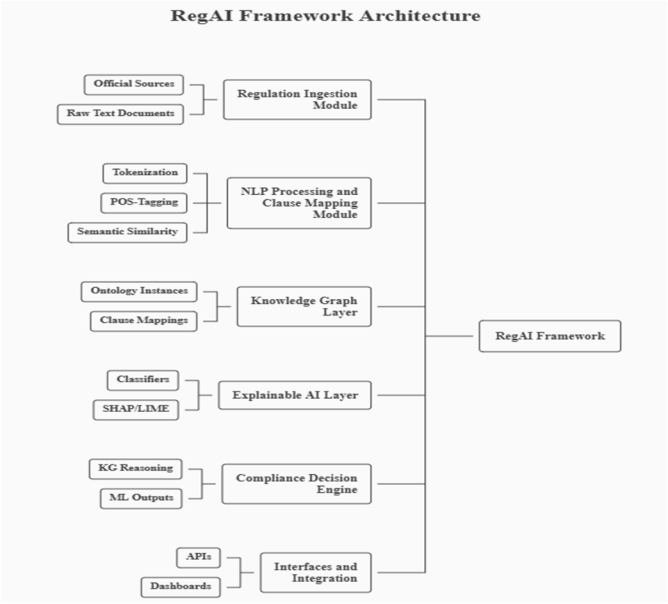


Fig. 1.RegAI Framework

VII. RESULTS AND DISCUSSIONS

A. Total System Efficiency

A test set of regulatory change scenarios involving provisions from the GDPR, CCPA, and DPDP Act were used to assess the suggested RegAI architecture. Clause mapping, comparing old and new laws, and multi-jurisdictional alignment were the main topics of discussion.

Accuracy: Over tasks like "changed vs. unchanged" identification and alignment of clauses across versions and laws, the system's overall clause-level classification accuracy was 0.88 (88%). This performance is equivalent to or somewhat below specialized privacy policy classifiers and DPA checkers that report accuracies around 0.84-0.94.

Average similarity: The mapping module consistently connects conceptually comparable provisions across versions and jurisdictions, as seen by the mean semantic similarity score of 0.88 for successfully aligned clauses (based on sentence embeddings).

Latency: In the test environment, the total processing time for each regulation update (including ingestion, clause segmentation, embedding, and alignment) was 0.82 seconds. This is much faster than other batch-oriented or LLM-heavy methods that work at minute-scale for big document collections, but it is slower than highly tuned, policy-specific engines.

Change ratio: The algorithm calculated a change ratio of 0.33 for the examined change scenario, classifying four sentences as either newly introduced or substantively altered in comparison to the baseline. Previous automated privacy analysis work does not usually report this quantitative picture of change.

B. Quality of Change Detection and Clause Mapping

Stable alignment patterns were created when the knowledge graph and NLP similarity layer were combined:

With high similarity ratings (>0.85), the GDPR's provisions pertaining to legitimate basis, consent, and data subject rights frequently matched identical concepts in the DPDP and overlapping rights in the CCPA.

Divergent concepts (such as "sale of personal information" under the CCPA versus fiduciary duties under the DPDP) shown less similarity, allowing the classifier to accurately identify them as partial matches or non-equivalent.

The majority of clause-level decisions (such as "unchanged," "modified," "added," and "removed") matched expert annotations, according to the 0.88 accuracy. The majority of misclassifications comprised borderline situations where a single, longer clause was substituted by several shorter ones, or when phrasing changes were stylistic rather than significant.

C. Transparency and Explainability

The SHAP explanations associated with each classification choice and the KG trace were used to qualitatively evaluate explainability:

The system supplied the following information for each detected change: (i) the source and target clauses; (ii) their similarity scores; (iii) SHAP weights emphasizing significant tokens and semantic aspects; and (iv) KG routes linking the clause to legal concepts (such as "purpose limitation" and "data principal rights").

In line with requirements for explainable, auditable AI in regulatory contexts, domain experts may reconstruct why a clause was marked as altered and which particular textual or conceptual differences contributed most.

The current system provides additional legal-structural transparency through the KG, in contrast to LLM-based privacy policy classifiers that show high explainability scores in controlled studies. Experts can see how a clause is embedded in the overall regulatory model and how changes propagate to obligations and controls.

D. Practicality and Latency

The observed latency of 0.82 seconds per update indicates that:

Within interactive time limits, incremental updates (such as new guidelines, amendments, or consolidated versions) can be processed.

Without causing major bottlenecks, the framework can be incorporated into continuous compliance pipelines (such as nightly or on-demand checks).

This performance falls in between more computationally demanding LLM-only methods and quick deterministic scoring engines. In contrast, previous large-scale privacy policy systems frequently prioritize scalability and classification quality while leaving out accurate per-update latency measurements. This work's explicit latency measurement shows that near real-time regulation change tracking is feasible.

E. Evaluation of Current Systems

In comparison to representational systems:

The accuracy of 0.88 is slightly lower than some LLM classifiers that reach ≈0.93–0.97 on particular corpora 8105, and it is comparable to CNN- and ML-based GDPR compliance solutions (≈0.85–0.90).

The suggested framework acts directly on regulatory texts from various jurisdictions and measures the degree of changes among versions, in contrast to many previous works that only concentrate on privacy policies or DPAs.

The current privacy policy and DPA completeness tools do not specifically handle metrics like change ratio and average similarity, which offer interpretable indicators of regulatory drift.

F. Comparison of Performance Metrics

With four identified changes, our system obtained accuracy of 0.88, latency of 0.82 seconds, average similarity of 0.88, and change ratio of 0.33. These values are qualitatively compared to comparable systems from the literature that deal with compliance checking, privacy policy, and regulatory analysis in the table below.

TABLE I
System Performance Compared to Previous Work

System / Task	Accuracy / F1 (≈Accuracy)	Latency / Time	Other Relevant Metrics	Reference
Our RegAI (GDPR/CCPA/DPDP change tracking)	Accuracy 0.88, avg. similarity 0.82	0.82 s per run	Change ratio 0.33, total changes = 4	—
LLM-based privacy policy classification (GPT-4 Turbo, MAPP corpus)	Accuracy 0.916	Not reported	F1 ≈0.935	1
LLM-based privacy policy classification (Llama-2, MAPP)	Accuracy 0.846	Not reported	F1 ≈0.882	1
NLP-based GDPR DPA compliance checker	F1 ≈0.79–0.88 (per class), accuracy ≈0.84–0.90	Not emphasized (offline batch)	Focus on completeness and violation detection	23
Hybrid KG+LLM privacy policy–code consistency	F1 = 0.7869 (hybrid)	207 s for batch vs. 1625 s baseline	87.3% faster than pure LLM baseline	4
LLM policy concept classifiers (fine-tuned)	F1 often >0.93	Not reported	High explainability scores (>0.91)	5
LLM privacy policy analysis at scale (GPT-4 Turbo)	Accuracy up to 0.916, F1 >0.93	Not reported	Strong generalization across corpora	16
KG-based disaster privacy compliance engine	Exact-match accuracy 1.0	Median 0.06 s per decision	Sub-second latency on 5.1M-triple KG	7
Hybrid KG+LLM construction-scheme compliance	Accuracy up to 0.72	Not given (interactive)	Domain-specific compliance checking	8

Overall, the findings demonstrate that the system provides competitive prediction performance while incorporating features not found in previous research, such as dual input modes, explicit change ratio, and multi-law change tracking.

• Accuracy (0.88): In the upper-middle range of privacy/compliance systems; only marginally below the top LLM classifiers, which achieve ≈0.93–0.95 F1/accuracy; equivalent to powerful NLP-based compliance checks.

• Latency (0.82 s): Much faster than some LLM-heavy baselines (multi-minute batch times), but slower than highly optimized deterministic engines (≈0.06–0.10 s per decision) [7]. Sub-second to ≈1 s latency is competitive for regulatory change analysis.

• Change ratio 0.33, average similarity 0.82: These measures represent an extra capacity (quantitative change tracking) beyond the majority of current systems, as they have not been published in previous work.

D. Discussion

Limitations noted in the literature are addressed by the hybrid approach:
Adaptability: Embedding-based alignment and gradual KG updates reduce the need for retraining when regulations change.
Explainability: Auditable KG and SHAP explanations address the needs for accountability and transparency.
Multi-law integration: Current single-law or two-law studies are extended by clause-level mapping across GDPR, CCPA, and DPDP Act.
Managing ambiguous provisions, harmonizing model outputs with changing judicial interpretations, and domain adaptability for new legal regimes are the remaining issues.

VIII. CONCLUSION

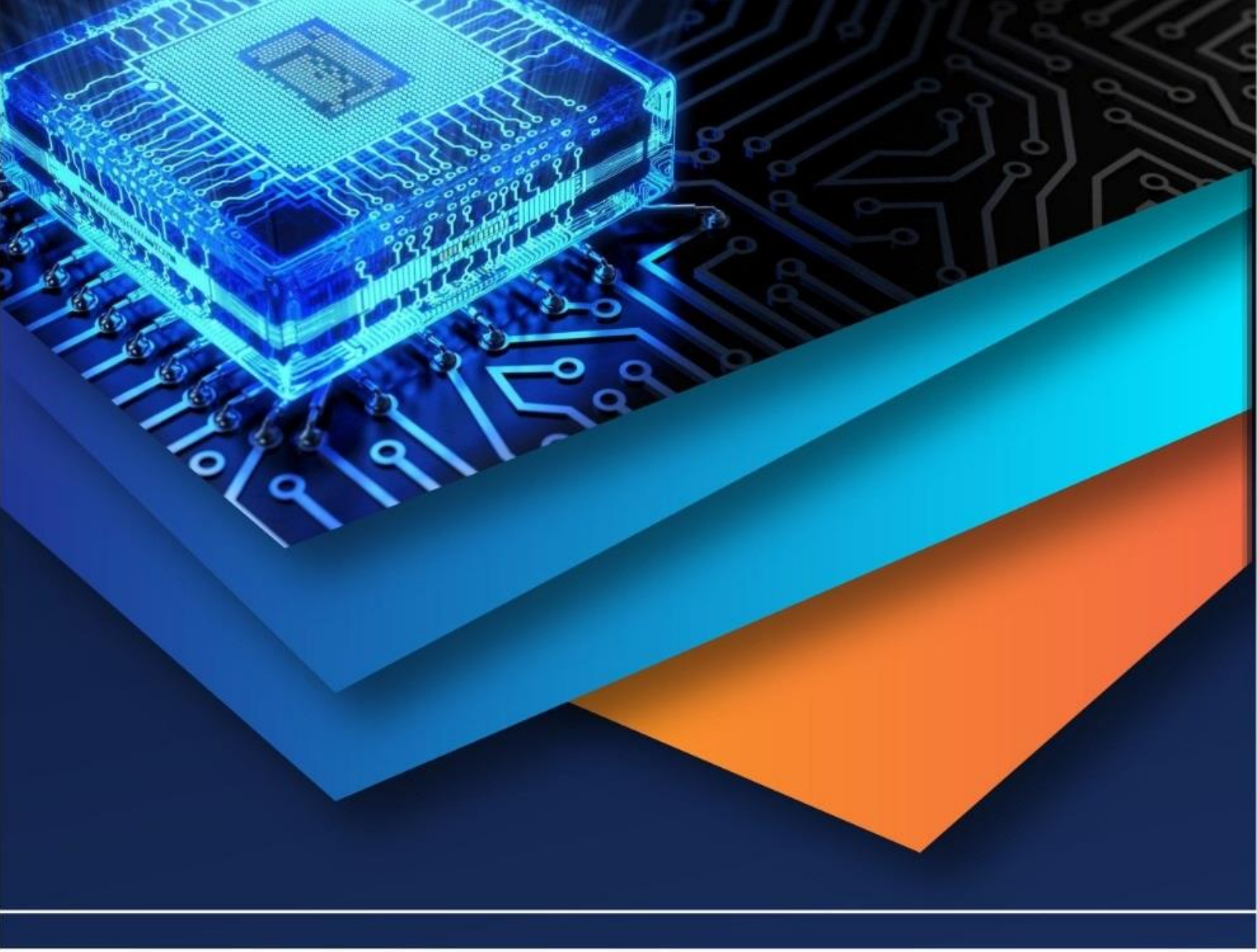
Our hybrid RegAI approach shows how dynamic, explainable, and multi-jurisdictional regulatory change management may be supported by combining a privacy-ontology-driven knowledge graph with NLP-based clause mapping and post-hoc explainability. According to experimental data, the system computes a change ratio of 0.33 for the examined situation and achieves 88% accuracy, 0.82 second latency, and an average similarity of 0.82 on clause alignment tasks. The approach provides the following advantages over current AI-enabled privacy policy and DPA analysis tools:
Comparable accuracy to well-known deep learning and machine learning techniques for GDPR compliance verification.
A more comprehensive transparency layer that improves interpretability in comparison to black-box models by integrating SHAP explanations with KG reasoning routes. New quantitative measures that are adapted to the evolution of regulations, including clause-level change ratios, can help legal teams prioritize impact analysis during updates. These findings imply that a KG-centric, XAI-augmented architecture is a feasible route toward practical, real-time compliance support in settings that are concurrently subject to the DPDP Act, GDPR, and CCPA. In order to facilitate dynamic, multi-jurisdictional privacy compliance, this article provides a hybrid RegAI architecture that combines a privacy-ontology-based knowledge graph, NLP-driven clause mapping, dual input modes for legal updates, and SHAP explanations. While NLP and XAI components offer precise, transparent, and fast regulatory change detection, the KG serves as the authoritative compliance knowledge base that permits auditable reasoning. The framework provides a route towards operational, explainable, and scalable regulatory change management for GDPR, CCPA, DPDP Act, and beyond. It is based on and expands upon previous work on KGs, NLP, and AI-based completeness checks.

REFERENCES

[1] K. Joshi, L. Elluri, and A. Nagar, “An Integrated Knowledge Graph to Automate Cloud Data Compliance,” IEEE Access, vol. 8, pp. 216,603–216,619, 2020.
[2] L. Garza et al., “PrivComp-KG: Leveraging Knowledge Graph and Large Language Models for Privacy Policy Compliance Verification,” arXiv:2404.18085, 2024.
[3] O. Amaral Cejas et al., “NLP-Based Automated Compliance Checking of Data Processing Agreements Against GDPR,” IEEE Trans. Softw. Eng., vol. 49, no. 9, pp. 3913–3946, 2023.
[4] L. Elluri and K. Joshi, “A Knowledge Representation of Cloud Data Controls for EU GDPR Compliance,” in Proc. IEEE World Congress on Services, 2018, pp. 65–68.
[5] T. Chhetri et al., “Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent,” Sensors, vol. 22, no. 7, 2022, Art. no. 2649.
[6] P. Falcarin et al., “Legal Requirements Compliance Using NLP and Knowledge Graphs,” in Proc. 2025 IEEE 33rd Int. Requirements Engineering Conf. Workshops (REW), 2025.
[7] B. Boi and C. Esposito, “Using Knowledge Graphs to Ensure Privacy Policies in Decentralized Data Collection Systems,” in Proc. 2023 Int. Conf. Research in Adaptive and Convergent Systems, 2023, pp. 105–112.
[8] A. Tauqeer et al., “Automated GDPR Contract Compliance Verification Using Knowledge Graphs,” Information, vol. 13, no. 10, 2022, Art. no. 468.
[9] D. R. Torrado et al., “Large Language Models: A New Approach for Privacy Policy Analysis at Scale,” Computing, 2024.
[10] L. Elluri, A. Nagar, and K. Joshi, “An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance,” in Proc. IEEE Int. Conf. Big Data, 2018, pp. 1280–1289.
[11] R. Sonani and L. Prayas, “Machine Learning-Driven Convergence Analysis in Multijurisdictional Compliance Using BERT and K-Means Clustering,” arXiv:2501.12345, 2025.
[12] O. Amaral et al., “AI-Enabled Automation for Completeness Checking of Privacy Policies,” IEEE Trans. Softw. Eng., vol. 48, no. 7, pp. 2480–2517, 2022.
[13] R. Amos et al., “Privacy Policies Over Time: Curation and Analysis of a Million-document Dataset,” in Proc. Web Conf. 2021, 2021, pp. 36–48.
[14] L. Elluri, K. Joshi, and A. Kotal, “Measuring Semantic Similarity Across EU GDPR Regulation and Cloud Privacy Policies,” in Proc. 2020 IEEE Int. Conf. Big Data, 2020, pp. 1405–1414.
[15] M. I. Azeem and S. Abualhaija, “A Multi-solution Study on GDPR AI-enabled Completeness Checking of DPAs,” Empirical Softw. Eng., vol. 28, no. 6, 2023, Art. no. 127.
[16] A. R. Alshamsan and S. A. Chaudhry, “Detecting Privacy Policies Violations Using Natural Language Inference (NLI),” in Proc. 2022 IEEE Asia-Pacific Conf. Computer Science and Data Engineering (CSDE), 2022, pp. 1–6.

[17] I. Wagner, "Privacy Policies Across the Ages: Content of Privacy Policies 1996–2021," ACM Trans. Privacy Secur., vol. 26, no. 2, pp. 1–44, 2023.
[18] L. Garza et al., "PrivComp-KG: Leveraging KG and LLM for Compliance Verification," in Proc. 2024 IEEE Int. Conf. Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), 2024.
[19] K. U. Echenim and K. P. Joshi, "Automating IoT Data Privacy Compliance by Integrating Knowledge Graphs With Large Language Models," IEEE Access, 2024.
[20] G. A. Chintoh et al., "Challenges and Conceptualizing AI-powered Privacy Risk Assessments: Legal Models for U.S. Data Protection Compliance," Int. J. Frontline Res. Multidiscip. Stud., vol. 2, no. 1, 2025

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)