*InView** AI Security Information

At Wolters Kluwer, we prioritize the security and privacy of your data in every aspect of *InView* AI systems. Our commitment to protecting your information is embedded in our development philosophy and operational practices. This document outlines the key security and privacy measures we have implemented to safeguard your valuable information.

** InView is a registered trademark*

Wolters Kluwer

InView
AI Discovery

AI Principles

At Wolters Kluwer, our products and services are based on a foundation of trust, transparency and responsibility – in line with our company values. Wolters Kluwer's AI Principles define Wolters Kluwer's approach and commitment to responsible AI and will guide the design, development and deployment of advanced technologies in helping our clients solve their most complex problems, today and well into the future.

See Wolters Kluwer Artificial Intelligence Principles Wolters Kluwer.

Data Protection

- **Data Encryption:** All data, including user interactions and conversation history, is encrypted at rest using AES-256 encryption. Our encryption keys are managed by AWS Key Management Service, ensuring secure key management practices.
- **Secure Transmission:** All internet traffic, both internal and external, is encrypted in transit using at least TLS 1.2 protocol, protecting your data as it moves between your device and our servers.
- **Data Privacy:** We do not use any customer data to train AI models. Your interactions with *InView* AI systems are used solely for the purpose of providing you with accurate and relevant legal information. We also ask that users do not provide any protected data in their prompts. However, if this occurs, relevant safeguards are in place to prevent the processing of protected data (see below).
- **Anonymization:** User interactions are anonymized for analytics and quality improvement processes. We do not store information that could identify which user generated specific interactions.
- **Protected data Detection and Redaction:** We have implemented protected data detection and redaction capabilities to further protect sensitive information.

Wolters Kluwer

InView
AI Discovery

AI Technology

- **Advanced Model:** *InView* AI systems utilize hosted Cloud Native closed train model, deployed in our private Azure OpenAI instance. This ensures that your queries are processed by one of the most advanced language models available, while maintaining strict control over data access and processing.
- **Secure Environment:** The AI models are deployed in protected, private cloud environments within Amazon AWS Europe, which are part of the secure Wolters Kluwer cloud infrastructure. These environments are subject to our comprehensive security controls. Agentic conversations are stored in the country of origin in a dedicated account, or in the closest AWS availability zone.
- **Isolated Processing:** Each user query is processed separately, generating a distinct transaction with our AI capabilities. This approach ensures that there's no cross-contamination of data between different users.
- **Opt-out of Microsoft Abuse Monitoring:** For our production workloads, we've opted out of Microsoft's automated content scanning, ensuring full control over data processing and enhanced privacy for all AI interactions.

Access Control and Security Measures

- **Least Privilege Access:** We implement strict access controls based on the principle of least privilege. Only authorized personnel with a genuine need have access to systems and data.

Transparency and Control

- **No Model Training:** We want to emphasize that your data is never used to train or fine-tune our AI models. *InView* AI systems are designed to provide you with information based on our extensive legal database, not to learn from your inputs.
- **Data Isolation:** We maintain logical separation between different firm accounts, ensuring that your data and interactions remain isolated and protected.
- **On-Demand Data Management:** While we anonymize and retain interaction data for quality improvement, we are actively investigating options for on-demand data purging to give you more control over your data.

Compliance and Security Practices

- **SOC 2 Principles:** While we have not yet undergone a formal SOC 2 audit, our systems and processes are designed to align with SOC 2 principles, focusing on security, availability, processing integrity, confidentiality, and privacy. We are committed to continuous improvement in these areas.
- **NIST Cybersecurity Framework:** Our development process and operational practices are aligned with the NIST Cybersecurity Framework.
- *InView* AI systems qualify as a limited-risk system under the **EU AI Act**.