

InView* AI Beveiligings- informatie

Bij Wolters Kluwer geven we prioriteit aan de beveiliging en privacy van uw gegevens in elk aspect van de *InView* AI-systemen. Onze toewijding aan het beschermen van uw informatie is ingebed in onze ontwikkelingsfilosofie en operationele praktijken. Dit document schetst de belangrijkste beveiligings- en privacy maatregelen die we hebben geïmplementeerd om uw waardevolle informatie te beschermen.

**InView is een geregistreerd handelsmerk*

AI Principles

Bij Wolters Kluwer zijn onze producten en diensten gebaseerd op een fundament van vertrouwen, transparantie en verantwoordelijkheid – in lijn met onze bedrijfswaarden.

De AI Principles van Wolters Kluwer definiëren de aanpak en toewijding van Wolters Kluwer aan verantwoorde AI en zullen de ontwerp-, ontwikkelings- en implementatieprocessen van geavanceerde technologieën begeleiden om onze klanten te helpen hun meest complexe problemen op te lossen, vandaag en in de toekomst.

Zie [Wolters Kluwer Artificial Intelligence Principles](#) | [Wolters Kluwer](#).

Gegevensbescherming

- ✓ **Gegevensversleuteling:** Alle gegevens, inclusief gebruikersinteracties en gespreks-geschiedenis, worden in rust versleuteld met AES-256 versleuteling. Onze versleutelingssleutels worden beheerd door AWS Key Management Service, wat zorgt voor veilige sleutelbeheerpraktijken.
- ✓ **Veilige transmissie:** Al het internetverkeer, zowel intern als extern, wordt tijdens de overdracht versleuteld met ten minste het TLS 1.2-protocol, waardoor uw gegevens worden beschermd terwijl ze tussen uw apparaat en onze servers worden verplaatst.
- ✓ **Gegeven privacy:** We gebruiken geen klantgegevens om AI-modellen te trainen. Uw interacties met *InView* AI-systemen worden uitsluitend gebruikt om u nauwkeurige en

relevante juridische informatie te bieden.

We vragen gebruikers ook om geen beschermde gegevens in hun prompts te verstrekken. Als dit echter gebeurt, zijn er relevante waarborgen om de verwerking van beschermde gegevens te voorkomen (zie hieronder).

- ✓ **Anonimiseren:** Gebruikersinteracties worden geanonimiseerd voor analyse- en kwaliteitsverbeteringsprocessen. We slaan geen informatie op die kan identificeren welke gebruiker specifieke interacties heeft gegenereerd.
- ✓ **Detectie en redactie van beschermde gegevens:** We hebben mogelijkheden voor detectie en redactie van beschermde gegevens geïmplementeerd om gevoelige informatie verder te beschermen.



Wolters
Kluwer

InView
AI Discovery

AI Technologie

- ✓ **Geavanceerd model:** InView AI-systemen maken gebruik van een gehost Cloud Native gesloten trainingsmodel, geïmplementeerd in onze privé Azure OpenAI-instantie. Dit zorgt ervoor dat uw vragen worden verwerkt door een van de meest geavanceerde taalmodellen die beschikbaar zijn, terwijl strikte controle over gegevens toegang en verwerking wordt gehandhaafd.
- ✓ **Veilige omgeving:** De AI-modellen worden geïmplementeerd in beschermde, privé cloud omgevingen binnen Amazon AWS Europe, die deel uitmaken van de veilige Wolters Kluwer cloud infrastructuur. Deze omgevingen zijn onderworpen aan onze uitgebreide beveiligingscontroles. Agentische conversaties worden opgeslagen in het land van herkomst in een toegewijd account, of in de dichtstbijzijnde AWS-beschikbaarheidszone.
- ✓ **Geïsoleerde verwerking:** Elke gebruikersvraag wordt afzonderlijk verwerkt, waardoor een afzonderlijke transactie met onze AI-mogelijkheden wordt gegenereerd. Deze aanpak zorgt ervoor dat er geen kruis

besmetting van gegevens tussen verschillende gebruikers plaatsvindt.

- ✓ **Opt-out voor Microsoft Abuse Monitoring:** Voor onze productie werklust hebben we ons afgemeld voor de geautomatiseerde inhoudsscan van Microsoft, waardoor volledige controle over gegevensverwerking en verbeterde privacy voor alle AI-interacties wordt gegarandeerd.

Toegangscontrole en beveiligingsmaatregelen

- ✓ **Toegang met minimale privileges:** We implementeren strikte toegangscontroles op basis van het principe van het minimale privileges. Alleen geautoriseerd personeel met een echte behoefte heeft toegang tot systemen en gegevens.

Transparantie en controle

- ✓ **Geen modeltraining:** We willen benadrukken dat uw gegevens nooit worden gebruikt om onze AI-modellen te trainen of te verfijnen. InView AI-systemen zijn ontworpen om u informatie te bieden op basis van onze

uitgebreide juridische database, niet om te leren van uw invoer.

- ✓ **Gegevensisolatie:** We handhaven logische scheiding tussen verschillende bedrijfsaccounts, waardoor uw gegevens en interacties geïsoleerd en beschermd blijven.
- ✓ **Gegevensbeheer op aanvraag:** Hoewel we interactiegegevens anonimiseren en bewaren voor kwaliteitsverbetering, onderzoeken we actief opties voor gegevensverwijdering op aanvraag om u meer controle over uw gegevens te geven.

Naleving en beveiligingspraktijken

- ✓ **SOC 2-principes:** Hoewel we nog geen formele SOC 2-audit hebben ondergaan, zijn onze systemen en processen ontworpen om in lijn te zijn met SOC 2-principes, met de nadruk op beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid en privacy. We zijn toegewijd aan voortdurende verbetering op deze gebieden.
- ✓ **NIST Cybersecurity Framework:** Ons ontwikkelingsproces en onze operationele praktijken zijn afgestemd op het NIST Cybersecurity Framework.