

SECURITY LEGAL MIND

Inleiding

Dit document beschrijft de technische en organisatorische beveiligingsmaatregelen die Legal Mind implementeert om persoonlijke gegevens te beschermen en de vertrouwelijkheid, integriteit en beschikbaarheid van de producten en diensten van Legal Mind te waarborgen. Meer details over deze maatregelen zijn op verzoek beschikbaar. Legal Mind behoudt zich het recht voor om deze maatregelen te herzien zonder voorafgaande kennisgeving, mits de bescherming van persoonlijke gegevens niet wezenlijk wordt verminderd.

Hoe Legal Mind Werkt

Legal Mind biedt een Software as a Service (SaaS)-platform voor juridische professionals, met modules zoals de Assistant Module, Dossier Management Module, Compliance Module en Document Drafter Module. Het platform is toegankelijk via webinterfaces en gebouwd op schaalbare cloudinfrastructuur, voornamelijk gehost door Microsoft Azure.

Sub-verwerkers

Legal Mind maakt onderscheid tussen huidige en toekomstige sub-verwerkers:

Huidige sub-verwerker:

Microsoft Azure: Hosting, infrastructuur en AI-tekstverwerking. Gegevens worden opgeslagen in Amsterdam, Nederland, in datacenters met geavanceerde fysieke beveiliging, zoals 24/7 bewaking, biometrische toegangscontroles en CCTV.

Auth0 (Okta): Identiteits- en toegangsbeheer. Gegevens van de EU-tenant worden opgeslagen in de AWS-regio eu-central-1, met een primair datacenter in Frankfurt (Duitsland) en fail-over in Dublin (Ierland). Deze AWS-datacenters beschikken over geavanceerde fysieke en organisatorische beveiliging, waaronder 24/7 bewakings-personeel, CCTV, meer-lagige biometrische en multi-factor toegangscontrole en geïntegreerde inbraak- en branddetectiesystemen. Gegevens blijven binnen de EU.

Toekomstige sub-verwerkers:

Legal Mind kan in de toekomst aanvullende sub-verwerkers inschakelen voor de verwerking van opdrachten met Large Language Models (LLM's), uitsluitend voor tijdelijke verwerking zonder langdurige opslag van gegevens. Deze sub-verwerkers moeten voldoen aan de volgende strikte kaders:

- Gevestigd in de Europese Unie als juridische entiteit, met voorkeur voor Nederland.
- ISO-gecertificeerd (ten minste ISO/IEC 27001).
- Gebruik van datacenters met geavanceerde fysieke beveiligingsmaatregelen, zoals 24/7 bewaking, biometrische toegangscontroles, CCTV en redundante systemen.
- Volledige naleving van de Algemene Verordening Gegevensbescherming (AVG) en andere relevante wet- en regelgeving.

De reden voor deze flexibiliteit is dat de snelle ontwikkeling van LLM-technologieën kan leiden tot de beschikbaarheid van sub-verwerkers die aanzienlijk betere prestaties of functionaliteiten bieden. Legal Mind behoudt de mogelijkheid om dergelijke toonaangevende technologieën te benutten, mits de bovengenoemde beveiligings- en AVG-normen strikt worden nageleefd. Legal Mind communiceert transparant over de inzet van toekomstige sub-verwerkers.

Bedrijfscontinuïteitsbeheer

Legal Mind waarborgt bedrijfscontinuïteit door dagelijkse back-ups van alle documenten in het Dossier Management Systeem (DMS), ook wel de "vault" genoemd. Deze back-ups vinden elke 24 uur plaats. Bij gekoppelde alternatieve DMS-systemen worden alleen de documenten geback-up't die handmatig zijn gesynchroniseerd naar de vault van Legal Mind. Dit betekent dat een dossier pas wordt geïndexeerd en opgenomen in de back-upcyclus van Legal Mind zodra de gebruiker het handmatig heeft gesynchroniseerd. Dit proces geeft de gebruiker controle over welke dossiers worden beveiligd en geback-up't in de vault, terwijl Legal Mind zorgt voor een betrouwbare en consistente back-up van deze gesynchroniseerde gegevens.

Beheer van Leveranciersrelaties

Legal Mind minimaliseert het gebruik van externe leveranciers door zoveel mogelijk in-house ontwikkeling toe te passen. Voor de weinige leveranciers die wel worden ingeschakeld, zoals Microsoft Azure, hanteert Legal Mind strikte beveiligings- en nalevingsnormen. Leveranciers worden grondig beoordeeld tijdens het inkoopproces en moeten voldoen aan alle toepasselijke wet- en regelgeving. Contracten bevatten strikte beveiligingsclausules, en Legal Mind voert kwartaallijkse audits uit om naleving te controleren.

Informatiebeveiligingsbeheer

Legal Mind beheert informatiebeveiliging via een robuust Information Security Management System (ISMS). We bouwen volledig op de ISO-gecertificeerde infrastructuur van Microsoft Azure, die voldoet aan standaarden zoals ISO/IEC 27001, SOC 1/2/3 en de AVG. Bij uitzondering worden alleen ISO-gecertificeerde diensten gebruikt, waarbij we zeer streng selecteren om de hoogste beveiligingsnormen te garanderen.

Systeemtoegangscontrole

Toegang tot Legal Mind-systemen is streng gereguleerd volgens het principe van minimale rechten. Alleen strikt noodzakelijke toegang wordt verleend. Multi-factor authenticatie (MFA) is verplicht voor alle systemen met persoonlijke of gevoelige gegevens. Toegang op hoog niveau (zoals administratieve of root-toegang) is beperkt tot een zeer klein aantal geautoriseerde personeelsleden, onderworpen aan continue monitoring en kwartaallijkse audits. Ongebruikte accounts worden direct gedeactiveerd.

Fysieke Toegangscontrole

Alle langdurige gegevensopslag van Legal Mind vindt exclusief plaats via Microsoft Azure-datacenters in Amsterdam (Schiphol). Deze datacenters zijn beveiligd met state-of-the-art fysieke beveiligingsmaatregelen, waaronder:

- 24/7 bewaking door getraind beveiligingspersoneel.
- Biometrische toegangscontroles, zoals vingerafdruk- en irisscanners.

- CCTV-camera's die alle in- en uitgangen en kritieke zones continu monitoren.
- Strikte toegangsprotocollen: alleen geautoriseerd personeel met geldige identificatie en voorafgaande goedkeuring mag het datacenter betreden.
- Bezoekers worden geregistreerd en continu begeleid door geautoriseerd personeel.
- Redundante systemen voor stroom, koeling en netwerken om operationele continuïteit te garanderen.

Deze datacenters zijn ISO/IEC 27001-gecertificeerd en ondergaan jaarlijkse audits door derden om de hoogste beveiligingsnormen te handhaven.

Toegangscontrole tot Gegevens

Legal Mind zorgt ervoor dat alleen geautoriseerde personen toegang hebben tot persoonlijke gegevens, passend bij hun rol en verantwoordelijkheden. Dit wordt gerealiseerd door:

- Rolgebaseerde toegangscontrole (RBAC): Toegang wordt verleend op basis van functierollen, met toepassing van het principe van minimale rechten.
- Wachtwoordbeleid: Sterke wachtwoorden zijn verplicht, met minimaal 10 karakters, inclusief hoofdletters, kleine letters, cijfers en speciale tekens. Wachtwoorden worden opgeslagen in een end-to-end versleutelde wachtwoordbeheerder. Wachtwoorden worden niet gedeeld via onbeveiligde kanalen zoals telefoon, chat, etc. Ze worden uitsluitend gedeeld via versleutelde methoden, zoals wachtwoordmanagers of beveiligde e-mails.
- Single Sign-On (SSO): Waar mogelijk wordt SSO met SAML 2.0 aangeboden voor veilige authenticatie.

Controle op Gegevenstransmissie

Legal Mind beveiligt de transmissie van persoonlijke gegevens door:

- Encryptie in transit: Gegevens in transit worden versleuteld met minimaal TLS 1.2, en waar mogelijk wordt TLS 1.3 gebruikt.
- Encryptie at rest: Gegevens at rest worden versleuteld met AES-256 of vergelijkbare algoritmen.
- Firewallbescherming: Firewalls blokkeren ongewenst verkeer en scheiden interne systemen in subnetwerken zonder directe externe toegang.

Invoercontrole

Legal Mind monitort en registreert toegang tot systemen om te traceren wie gegevens heeft ingevoerd, gewijzigd of verwijderd. Dit omvat:

- Logging: Alle systeemactiviteiten worden gelogd met timestamps en gebruikersidentificatie, centraal opgeslagen.
- Bewaartermijn logs: Beveiligingslogs worden minimaal 12 maanden bewaard.

Beschikbaarheidscontrole

Legal Mind waarborgt de beschikbaarheid van gegevens door:

- Dagelijkse back-ups: Back-ups van de DMS "vault" worden elke 24 uur uitgevoerd.
- Redundantie: Gebruik van Microsoft Azure's redundante systemen voor stroom, netwerken en koeling.
- Patchmanagement: Systemen worden tijdig gepatcht om kwetsbaarheden te minimaliseren.

Risicobeheer

Legal Mind hanteert een proactieve aanpak voor risicobeheer door:

- Periodieke risicobeoordelingen: Jaarlijkse evaluaties van beveiligingsrisico's en naleving.
- Beveiligingstraining: Medewerkers ontvangen regelmatige training over informatiebeveiliging en gegevensbescherming.
- Rapportering: Regelmatige updates aan het management over beveiligingsstatus en naleving.

Operationele Beveiliging

Legal Mind beveiligt haar operationele systemen door:

- Antivirus en antimalware: Actieve monitoring en bescherming tegen kwaadaardige software.
- Patchmanagement: Regelmatige installatie van beveiligingsupdates.
- E-mailbeveiliging: Gebruik van spamfilters en malwarebescherming voor e-mails.

Beveiliging met Betrekking tot Personeel

Legal Mind zorgt ervoor dat personeel voldoet aan beveiligingsnormen door:

- Geheimhoudingsverklaringen: Alle medewerkers ondertekenen een geheimhoudingsovereenkomst.
- Beveiligingstraining: Periodieke training over informatiebeveiliging en privacy.
- Achtergrondchecks: Redelijke controles op medewerkers, binnen wettelijke grenzen.

Bewaring van Persoonsgegevens

Legal Mind bewaart persoonlijke gegevens conform klantinstructies en wettelijke vereisten. Na beëindiging van de overeenkomst worden gegevens veilig verwijderd of geretourneerd, tenzij wettelijk anders vereist.

AI & Data Management

Wij stellen de security en vertrouwelijkheid van klantdata centraal, zeker bij het gebruik van Large Language Models (LLM's). Onze partnership met Microsoft Azure illustreert onze inzet voor cutting-edge AI en maximale dataveiligheid.

Ontwerpprincipes

Onze AI-principes zijn eenvoudig:

1. Alleen bekende, betrouwbare en veilige providers worden gebruikt.
2. Wij implementeren uitsluitend AI-modellen die géén data opslaan.
3. Contractuele garanties dat providers geen data gebruiken voor training.

Data security

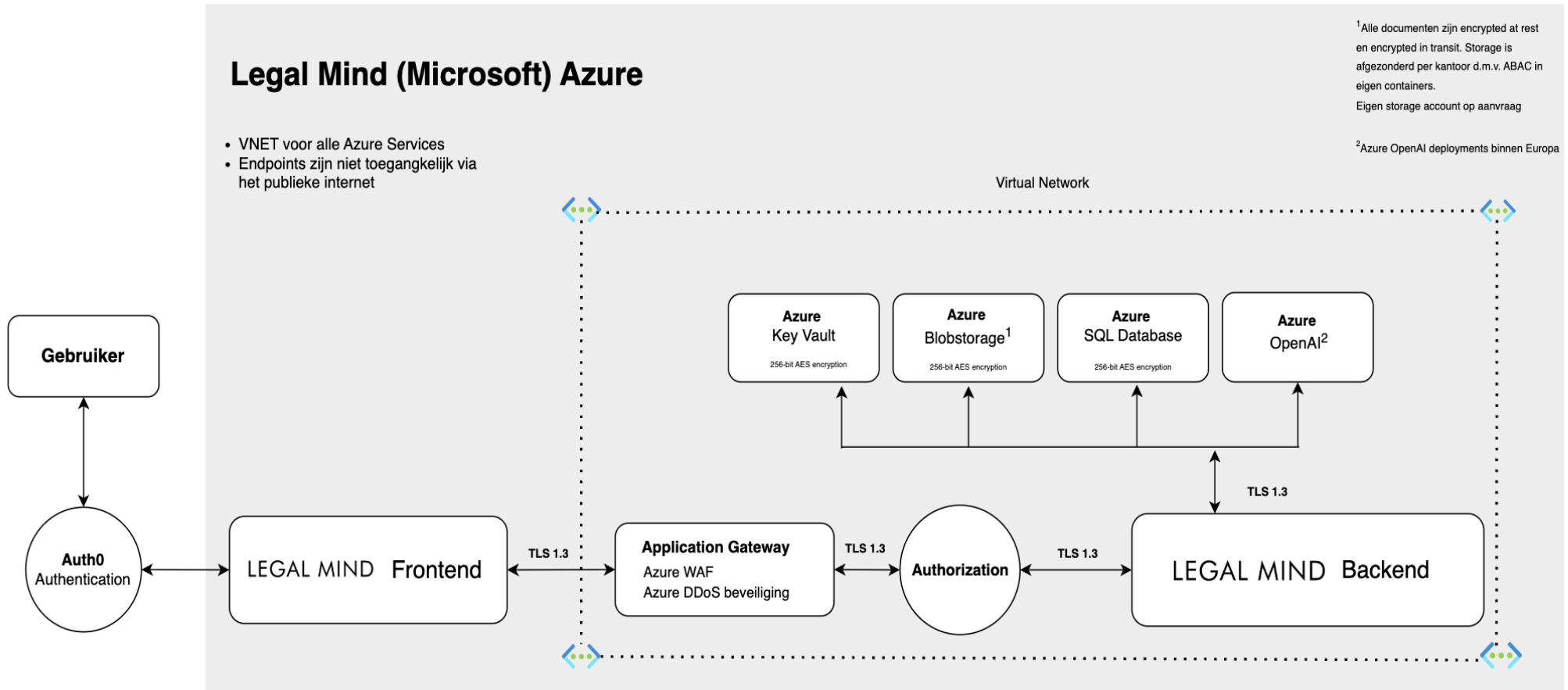
1. **Gegevensisolatie:** Uw gegevens zijn veilig geïsoleerd en worden niet gedeeld met andere klanten of opgeslagen bij onze AI-modelleveranciers. Deze aanpak zorgt voor een sterke bescherming tegen ongeautoriseerde toegang. *zie diagram
2. **Modeltraining en verbetering:** Legal Mind gebruikt uw gegevens niet voor training, fine-tuning of automatische verbetering van AI-modellen. Dit beleid geldt voor alle gebruikte AI-modellen.
3. **Encryptie:** Alle gegevensinteracties worden versleuteld om vertrouwelijkheid en integriteit te waarborgen, zodat wordt voldaan aan de industriestandaarden.

Aanpassing aan Technologische Veranderingen

Legal Mind erkent dat de snelle ontwikkelingen in de markt kunnen leiden tot veranderingen in de gebruikte technieken en technologieën. Om de veiligheid en effectiviteit van onze diensten te waarborgen, kan het nodig zijn om deze maatregelen aan te passen. Klanten worden tijdig en duidelijk geïnformeerd over dergelijke aanpassingen. Deze aanpassingen zijn bedoeld om de beveiliging te verbeteren of om te voldoen aan nieuwe wettelijke vereisten en zullen geen afbreuk doen aan de overeengekomen beveiligingsnormen.

Security- en infrastructuurdiagram

Legal Mind: IT Security protocol diagram 2025



Datascheidingsdiagram

