Een AI-leverancier beoordelen: vragen en bewijs voor het advocatenkantoor

Voor Nederlandse advocaten en kantoren. Begin met één concrete werkzaamheid, bijvoorbeeld het ordenen van fictieve correspondentie. Een overtuigende demonstratie zegt weinig over geschiktheid voor vertrouwelijke dossiers. Vraag om bewijs dat hoort bij de dienst, instellingen en toepassing die uw kantoor daadwerkelijk overweegt.

De NOvA-aanbevelingen over AI behandelen onder meer deskundigheid, geheimhouding, leveranciersafspraken en handmatige controle. Het zijn aanbevelingen; de wettelijke AVG-beoordeling blijft een afzonderlijke stap. Dit algemene hulpmiddel geeft geen advies over een concreet dossier en bewijst geen naleving.

Leg het onderzoek vast

Noteer bij ieder antwoord: **ontvangen bewijs, datum, bevinding, open punt en verantwoordelijke**. Bewaar de toepasselijke voorwaarden en relevante instellingen bij het bestaande inkoop- of risicodossier. Een onbeantwoorde vraag vraagt om een beperking of vervolgonderzoek.

1. Welke werkzaamheid kan het kantoor verantwoord ondersteunen?

Vraag om een beschrijving van mogelijkheden, beperkingen en wijzigingen. Laat de leverancier een representatieve opdracht uitvoeren met fictieve gegevens, inclusief een onvolledige vraag. Leg vast welke taken, medewerkers en gegevenscategorieën u onderzoekt. Beoordeel samenvatten, juridisch onderzoek en concepten afzonderlijk.

2. Waar gaan invoer en uitvoer heen?

Vraag een gegevensstroomschema met documenten, zoekopdrachten, antwoorden, logbestanden, reservekopieën, ondersteuning en koppelingen. Wie ontvangt welke informatie, waar en waarom? De NOvA beveelt aan invoer en uitvoer binnen de kantooromgeving te houden. Vraag hoe de voorgestelde inrichting dat ondersteunt. Een lokale installatie sluit externe verwerking niet uit; een opslaglocatie beschrijft evenmin alle toegangswegen.

3. Welke vertrouwelijke informatie mag worden ingevoerd?

Onderzoek geheimhoudingsafspraken, menselijke inzage en doorverstrekking. De NOvA raadt af vertrouwelijke of cliëntgegevens in publieke AI-modellen in te voeren. Leg concrete uitsluitingen vast. Haar aanbeveling om cliënttoestemming te vragen voor AI-gebruik in het dossier vervangt geen AVG-grondslag en lost de bescherming van gegevens van wederpartijen of derden niet vanzelf op. Beoordeel geheimhouding en verschoningsrecht afzonderlijk.

4. Welke AVG-rol vervult iedere partij?

Vraag per verwerkingsdoel wie doel en middelen bepaalt: dienstverlening, accountbeheer, beveiliging en eventueel hergebruik kunnen verschillen. Art. 4 onder 7 en 8 AVG onderscheidt verwerkingsverantwoordelijke en verwerker. Art. 28 geldt wanneer verwerking namens een verwerkingsverantwoordelijke plaatsvindt. Een externe AI-leverancier is niet voor elke activiteit automatisch verwerker. Vraag waar toepasselijk om de volledige verwerkersafspraken.

5. Wat gebeurt er na het antwoord?

Vraag bindende afspraken over modeltraining, verbetering van de dienst, menselijke beoordeling, bewaartermijnen en verwijdering. Controleer of instellingen overeenkomen met de overeenkomst. Wie kan ze wijzigen? Geen training betekent op zichzelf niet dat documenten, antwoorden of logbestanden niet worden bewaard of ingezien.

6. Welke andere partijen en landen zijn betrokken?

Vraag om de betrokken dienstverleners, hun werkzaamheden, locaties en wijzigingsprocedure. Onderzoek ook toegang door ondersteuning op afstand. Leg vast of doorgifte buiten de Europese Economische Ruimte speelt en welke beoordeling en waarborgen daarvoor nodig zijn. Een Europees datacentrum geeft daarover geen volledig antwoord.

7. Welke risicoanalyse past bij dit gebruik?

Vraag informatie over betrokken personen, gegevens, schaal en gevolgen van fouten. Gepseudonimiseerde gegevens zijn niet noodzakelijk anoniem. Beoordeel bijzondere categorieën persoonsgegevens en strafrechtelijke gegevens afzonderlijk: art. 9 en 10 AVG hebben verschillende regimes. De NOvA beveelt een DPIA bij persoonsgegevens aan; de wettelijke verplichting uit art. 35 AVG geldt bij waarschijnlijk hoog risico. Leg beide afwegingen herkenbaar vast.

8. Welke beveiliging werkt in de praktijk?

Vraag bewijs over toegangsrechten, scheiding tussen kantoren en dossiers, versleuteling en incidentafhandeling. Test met fictieve informatie of een onbevoegde medewerker werkelijk wordt geweigerd en of vertrokken medewerkers toegang verliezen. Benoem wie een incidentmelding ontvangt en welke informatie het kantoor nodig heeft voor zijn eigen beoordeling.

9. Kan een advocaat het resultaat controleren?

Vraag om herleidbare documentverwijzingen, bronlinks, rechtsgebiedkeuze en informatie over actualiteit. Test een ontbrekende bron en een onjuiste aanname. De NOvA beveelt handmatige controle van citaten, rechtspraak en feiten aan. Leg vast wie die controle uitvoert en wanneer een antwoord buiten gebruik blijft.

10. Kan het kantoor verantwoord vertrekken?

Vraag om uitvoerformaten, opzegvoorwaarden en verwijderingsafspraken voor alle kopieën. Test een export met fictief materiaal en open die buiten de dienst. Bepaal welke informatie in het eigen dossier moet blijven. Herbeoordeel bij gewijzigde voorwaarden, ontvangers, modellen, koppelingen of werkzaamheden; verleen geen algemene goedkeuring op basis van dit leveranciersgesprek.

Versie 1.0.0, eerste uitgave. Recht en aanbevelingen gecontroleerd: 8 november 2026. Inhoudelijk beoordeeld: 8 november 2026. Volgende beoordeling: 8 februari 2027. Controleer vóór toepassing of er een nieuwere uitgave of gewijzigde bron is.