AI Beleid Stellicher Advocaten

1. Doel en reikwijdte
Dit beleid is opgesteld om duidelijke richtlijnen te bieden voor het gebruik van kunstmatige intelligentie (AI) binnen ons kantoor. Het gaat daarbij met name om de inzet van AI bij het verzamelen van juridische informatie en antwoorden, het analyseren van bronnen en het opstellen of redigeren van juridische documenten en adviezen.

Het beleid geldt voor alle medewerkers, waaronder advocaten, advocaat-stagiairs, juridisch medewerkers en ondersteunend personeel. Doelstellingen van dit beleid zijn: - Het waarborgen van vertrouwelijkheid en geheimhouding. - Het correct naleven van de AVG en andere privacywetgeving. - Het bieden van praktische kaders voor veilig gebruik van AI-toepassingen. - Het waarborgen dat kwaliteit en verantwoordelijkheid te allen tijde bij de medewerkers van kantoor liggen.

2. Uitgangspunten
1. Geheimhouding en integriteit: Advocaten zijn op grond van de Advocatenwet en de Gedragsregels verplicht tot absolute geheimhouding van cliëntinformatie. Het gebruik van AI mag deze geheimhouding niet schenden of in gevaar brengen. Dit betekent dat instellingen in gebruikte AI-systemen, waaronder ChatGPT, zo moeten worden ingericht dat (ingevoerde) data niet worden hergebruikt, niet zichtbaar worden voor derden en uitsluitend dienen ter ondersteuning van de lopende sessie.

2. Rechtszekerheid en betrouwbaarheid: AI is een hulpmiddel, geen vervanging van juridische expertise. Iedere output van AI moet zorgvuldig en kritisch worden getoetst door een advocaat voordat deze intern of extern wordt gebruikt. Daarnaast geldt dat in alle gevallen verwijzingen naar literatuur en jurisprudentie die door AI worden aangereikt, zorgvuldig moeten worden gecontroleerd op juistheid, actualiteit en relevantie, alvorens deze te gebruiken in adviezen, processtukken of interne documenten.

3. Transparantie en verantwoording: Cliënten en collega's moeten erop kunnen vertrouwen dat duidelijk is wanneer AI is toegepast. Iedere medewerker heeft een informatieplicht richting het kantoor en collega's, indien AI-gebruik van wezenlijke invloed is geweest op de inhoud van een document of advies. 4. Privacy en gegevensbescherming. De Algemene Verordening Gegevensbescherming (AVG) en aanverwante regelgeving zijn altijd leidend. AI mag uitsluitend worden ingezet binnen de kaders van de AVG en alleen als de veiligheid van gegevens is gewaarborgd.

3. Gebruik van AI in de praktijk
1. Grondslag: Verwerking van persoonsgegevens via AI-tools is alleen toegestaan op basis van een vooraf vastgestelde grondslag. Voor advocaten geldt dat een opdrachtbevestiging door de cliënt moet zijn getekend voordat persoonsgegevens in een

goedgekeurde AI-tool kunnen worden verwerkt. Waar mogelijk wordt gewerkt met inachtneming van dataminimalisatie (art. 5 AVG).

2. Uploaden en delen van informatie: Het is verboden vertrouwelijke of tot personen herleidbare gegevens in externe AI-toepassingen te uploaden zonder expliciete toestemming van de verantwoordelijke partner. Bij voorkeur worden gegevens geanonimiseerd of geabstraheerd voordat deze in een AI-toepassing worden ingevoerd. Documenten met bijzondere persoonsgegevens (zoals gezondheidsgegevens, religieuze overtuiging, strafrechtelijke informatie) mogen nooit zonder voorafgaand overleg en goedkeuring via AI-toepassingen worden verwerkt.

3. Toepassingsgebieden: AI kan worden gebruikt voor alle (dossier)werkzaamheden, waaronder onderzoekswerk, samenvatten van arresten, analyseren van publiek beschikbare wetteksten of literatuur, Inhoudelijke dossieranalyse, het vinden van alternatieve juridische argumentaties of tegenargumenten en productie concept tekst voor processtukken, adviezen en overeenkomsten.

4. Niet toegestane toepassingen: Het rechtstreeks overnemen van AI-output in juridische adviezen of processtukken zonder inhoudelijke toetsing. Indien AI is gebruikt voor vragen die liggen buiten de Nederlandse rechtssfeer of anderszins via AI verkregen informatie zonder de in dit beleid genoemde controles gericht op juistheid en kwaliteit worden doorgestuurd aan cliënten, wordt expliciet vermeld dat het een (uitsluitend) via AI gegenereerd product is. Uitgangspunt is dat dit zo min mogelijk gebeurt. Het verwerken van cliëntgegevens in accounts of toepassingen anders dan goedgekeurde AI tools.

4. Instellingen en gebruik van AI-toepassingen

Alleen tools op de lijst met goedgekeurde AI-tools mogen worden gebruikt. Aan dit beleid zal een lijst worden gehecht met de goedgekeurde AI tools. Nieuwe toepassing die worden goedgekeurd worden aan de lijst toegevoegd.

Voor ChatGPT geldt dat uitsluitend het centraal beheerde zakelijke account (Team/Enterprise of een vergelijkbaar niveau met een Data Processing Addendum) wordt gebruikt. Individuele (privé) ChatGPT Pro-abonnementen die niet onder centraal IT-beheer vallen, zijn niet toegestaan voor gebruik waarbij persoonsgegevens of dossiergegevens worden ingevoerd. Algemene juridische vragen waarbij geen gebruik wordt gemaakt van dossier- of persoonsgegevens mogen wel in (eigen) AI-tools worden gesteld, maar er wordt bij voorkeur alleen gewerkt in de goedgekeurde AI-tools van kantoor.

Zeno en overige goedgekeurde juridische tools mogen worden gebruikt. Gebruikers mogen de verwerkingsinstellingen (zoals hierna nader geduid) die zien op gebruik en het bewaren van documenten, data en output nooit zelfstandig wijzigen.

Een advocaat of medewerker die een niet op de lijst staande AI tool wil gebruiken, meldt dit vooraf aan de Tech Tascforce binnen kantoor of de IT verantwoordelijke voor een risicobeoordeling.

Alle AI-toepassingen die binnen het kantoor worden gebruikt, dienen zodanig te worden geconfigureerd dat geheimhouding, vertrouwelijkheid en naleving van privacyregels maximaal worden gewaarborgd. Het kantoor zal, waar mogelijk, per toepassing die als goedgekeurde AI-tool wordt gebruikt, de instellingen centraal regelen of, indien dat niet mogelijk is, aangeven welke instellingen gehanteerd moeten worden. Iedere medewerker is verplicht deze richtlijnen te volgen en geen gebruik te maken van AI-tools met instellingen die hiervan afwijken.

Voor iedere AI-tool gelden de volgende uitgangspunten:

1. De model opdrachtbevestigingen zijn aangevuld met een AI-gebruiksclausule die cliënten informeert over het (mogelijke) gebruik van AI-tools in hun dossier, waarmee toestemming van een cliënt voor verwerking van diens gegevens via een AI-tool schriftelijk wordt vastgelegd in het dossier.

2. Data-sharing uitschakelen: Documenten en gegevens die worden ingevoerd, mogen nooit worden gebruikt voor training of verbetering van de AI-tool of het onderliggende LLM. In Zeno en het ChatGPT Enterprise-abonnement van kantoor is dit een standaardinstelling. Controleer bij ChatGPT periodiek of de optie “Chatgeschiedenis en training” nog steeds is uitgeschakeld.

3. Opslag beperken: Gebruik uitsluitend kantooraccounts en sla documenten niet permanent op binnen de ChatGPT-omgeving. Bewaar relevante output uitsluitend binnen interne kantoorsystemen.

4. Beveiligde toegang: Zorg dat alle accounts zijn voorzien van sterke wachtwoorden en voor externe toegang – via telefoon of eigen laptop – met tweefactorauthenticatie. Gebruik geen privé-accounts met dossiergegevens.

5. Gegevensminimalisatie: Voer enkel die gegevens in die strikt noodzakelijk zijn om de gewenste ondersteuning te verkrijgen. Voorkom zoveel als mogelijk nodeloze invoer van persoonsgegevens of zaak-specifieke vertrouwelijke details. Bij gebruik van niet goedgekeurde AI-tools is invoer van deze gegevens niet toegestaan. Dit laatste geldt als het delen van vertrouwelijke informatie met een derde en kan een schending van art. 11a Advocatenwet en gedragsregel 3 opleveren.

6. Controle en logging: Noteer in het dossier of en hoe een AI tool is gebruikt. Neem vragen en output die zijn verwerkt in processtukken of adviezen aan cliënten zoveel mogelijk op in het dossier in Basenet, zodat altijd transparantie bestaat binnen het kantoor. Voor stagiaires geldt daarbij hetgeen is opgenomen in onderdeel 6 van dit beleid.

7. Afsluiten dossier: Indien een dossier wordt gesloten en gearchiveerd, worden ingevoerde documenten en data betrekking hebbende op dat dossier, met inbegrip van

vragen en antwoorden, uit alle AI-tools verwijderd door de behandelend advocaat. Indien er een noodzaak is om deze (deels) te bewaren, worden deze documenten of data (voor zover nog nodig) geëxporteerd en opgeslagen in het dossier zelf.

5. Omgang met prompts voor AI-toepassingen

Prompts die door medewerkers worden gebruikt om door de cliënt aangeleverde documenten en gegevens te analyseren of beoordelen met behulp van AI-toepassingen, dienen altijd te worden opgeslagen in het bijbehorende dossier. Dit zorgt voor transparantie, controleerbaarheid en herleidbaarheid van het gebruik van AI in juridische werkzaamheden. Het vastleggen van prompts draagt bij aan de kwaliteitsbewaking en maakt het mogelijk om achteraf te verifiëren welke input is gebruikt om tot bepaalde output te komen.

Prompts die zijn opgesteld en gebruikt voor het genereren van specifieke juridische content, waaronder contracten, processtukken en adviezen, kunnen aanvullend worden opgeslagen in de speciaal daarvoor ingerichte promptdossiers in Basenet. Dit stelt het kantoor in staat om een centrale en gestructureerde database voor het gebruik van AI-gebruik bij te houden.

6. Training en controle

Medewerkers krijgen bij indiensttreding en periodiek een verplichte AI-training. Daarbij wordt naast de vaardigheden voor het gebruik van AI-tools, ten minste aandacht besteed aan de volgende onderwerpen:

- De geldende versie van dit beleid.
- Herkenning van hallucinaties en onjuiste output.
- De regels rond bijzondere persoonsgegevens, en de transparantieverplichtingen van art. 50 AI Act.

Er zal periodiek een interne audit plaatsvinden om te controleren of medewerkers dit beleid juist hebben toegepast en of er geen vertrouwelijke informatie in externe systemen is beland. Medewerkers zijn verplicht iedere (mogelijke) datalek of onjuist gebruik van AI onmiddellijk te melden aan de IT functionaris of de aangewezen partner.

Iedere medewerker meldt een (mogelijk) datalek of onjuist AI-gebruik onmiddellijk aan de IT verantwoordelijke of de aangewezen partner. De IT functionaris beoordeelt binnen 24 uur of een meldplicht aan de Autoriteit Persoonsgegevens binnen de wettelijke termijn van 72 uur aan de orde is, of dat er sprake is van een schending van de geheimhouding.

Voor advocaat-stagiairs gelden de navolgende specifieke regels:

- De mate waarin AI-tools door advocaat-stagiairs wordt gebruikt, wordt afgestemd met de patroon.

- Advocaat-stagiairs moeten bij ieder aangeleverd stuk aangeven of AI is gebruikt en, zo ja, in welke mate.
- Indien AI is gebruikt, moet duidelijk worden vermeld welke onderdelen door AI zijn gegenereerd (bijvoorbeeld “concept-structuur opgesteld met behulp van AI, inhoud volledig herzien door stagiair”).
- Voor opleidingsdoeleinden wordt stagiairs geleerd om kritisch te evalueren: AI-output mag nooit ongefilterd worden doorgegeven.

Iedere advocaat is zelf verantwoordelijk voor naleving van dit beleid in eigen dossiers of bij behandeling van dossier van andere advocaten. Een patroon is verantwoordelijk voor het toezicht op AI-gebruik door hun stagiairs en stemt dat zoveel mogelijk met die stagiaire af.

Het bestuur kan disciplinaire maatregelen nemen indien regels worden overtreden, variërend van een waarschuwing tot uitsluiting van AI-gebruik of andere arbeidsrechtelijke maatregelen.

Het beleid wordt jaarlijks geëvalueerd en zo nodig aangepast aan nieuwe technologische en juridische ontwikkelingen.

7. Governance en rollen.

De Tech Tascforce zal samen met de IT-verantwoordelijke het toezicht houden op toepassing en uitvoering van dit beleid, en:

- stelt jaarlijks de lijst van toegestane en door haar goedgekeurde AI-toepassingen vast.
- behandelt meldingen van incidenten en geconstateerd afwijkend gebruik.
- rapporteert jaarlijks aan het bestuur.

Bij twijfel of vragen over de toepassing dient contact te worden opgenomen met het bestuur of iemand van het AI-comité.

Dit herziene beleid treedt in werking op 16 november 2026.